JUDGE CASTEL

DOC

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

'08 CIV 5689

AMIDAX TRADING GROUP, on behalf of itself and all others similarly situated,

Plaintiffs,

v.

S.W.I.F.T. SCRL, S.W.I.F.T. Pan-Americas Inc., S.W.I.F.T., Inc., John Snow, in his personal and professional capacities, Stuart Levey, in his personal and professional capacities, United States Department of the Treasury, George W. Bush, in his personal and professional capacities, Central Intelligence Agency, Richard Cheney, in his personal and professional capacities, George Tenet, in his personal and professional capacities, Michael Hayden, in his personal and professional capacities, Henry M. Paulson, Jr., in his personal and professional capacities,

Defendants

Complaint for Damages, Declaratory, and Injunctive Relief

JURY TRIAL DEMANDED

CLASS ACTION

COMPLAINT

Plaintiffs, by their counsel, individually and on behalf of all others similarly situated, as and for their Complaint against Defendants assert upon information and belief as follows:

PRELIMINARY STATEMENT OF THE CASE

1. On June 23, 2006, then-Secretary of the Treasury John Snow held a press conference. During that press conference, Secretary Snow said:

> "We started with a narrowly targeted subpoena. That's how we started. SWIFT wasn't able to respond to a narrowly targeted subpoena. Remember, the subpoena has to be tied to terrorism. This is not a subpoena that gives us access to data that doesn't have linkages to terrorism. Once the data was available to us, we targeted leads, intelligence leads, in going in and making inquiries on the data. So we started with really narrowly crafted subpoenas, all tied to terrorism SWIFT wasn't able to provide us… to respond to our request to provide us with the answers to the subpoena because they didn't have the ability to extract the particular information from their

broad database ***so they said to us, "We'll give you all the data". They knew from the beginning that that wasn't our objective, to get all the data.*** Our objective was this carefully targeted… on leads… on intelligence leads leading to terrorism and ***over time*** we've worked together. It's been a very cooperative effort ***to narrow the scope of our subpoena*** and we have. We've narrowed it in terms of the number of fields, that is, the number of areas in which we get access to their financial messages and we've narrowed the geographical scope." (Emphases added).

A DVD containing video webcast of this press conference is attached as "Exhibit A". The webcast can also be viewed at the United States Treasury Department's website at http://www.yorkmedia.com/treasury/webcasts2006.html (last accessed June 23, 2008) by scrolling down to "June 23, 2006 Terrorist Finance Tracking Program" and clicking on the link to either "View in Real Player Format" or "View in Windows Media". A .pdf version of the webpage containing a link to the conference is attached as "Exhibit B".

2. Earlier that day, the *New York Times*, the *Los Angeles Times*, and the *Wall Street Journal* ran stories describing a "Terrorist Finance Tracking Program (the 'TFTP')" involving Defendant SWIFT's disclosure to the United States Government of "financial records… involving tens of thousands of Americans and others in the United States". ("Exhibit C", the *New York Times*, June 23, 2006, "Bank Data Sifted in Secret by U.S. to Block Terror" by Eric Lichtblau and James Risen). This article contained a reference to an unnamed person close to the operation as saying, "At first, they (the U.S. Government) got everything - the entire SWIFT database."

3. The following day, June 24, 2006, the *New York Times* published a follow-up article quoting Secretary Snow as saying, "So they (SWIFT) said, 'We'll give you all the data.'" ("Exhibit D", the *New York Times*, June 24, 2006, "Cheney Assails Press on Report on Bank Data" by Sheryl Gay Stolberg and Eric Lichtblau).

4. Upon information and belief, SWIFT's disclosures described above by Secretary Snow were made in violation of the United States Constitution, the United States Right to Financial Privacy Act, and various state laws, consumer fraud, and consumer protection statutes.

5. Plaintiff is suing to stop this illegal conduct and hold Defendants responsible for their illegal conduct.

JURISDICTION AND VENUE

6. This court has subject matter jurisdiction over the federal claims pursuant to Article III of the United States Constitution, 28 U.S.C. §1331, 28 U.S.C. §2201, 12 U.S.C. §3416, 12 U.S.C. § 3416, 12 U.S.C. §3417, 12 U.S.C. §3418, and over the state claims pursuant to 28 U.S.C. §1332 and 28 U.S.C. §1367.

7. Plaintiffs are informed, believe and thereon allege that Defendants have sufficient contacts with this district generally and, in particular, with the events herein alleged, that Defendants are subject to the exercise of jurisdiction of this court over the person of each Defendant and that venue is proper in this judicial district pursuant to 28 U.S.C. §1391.

8. Plaintiffs are informed, believe and thereon allege that, based on the places of business of Defendants identified above and/or on the national reach of Defendants, a substantial part of the events giving rise to the claims herein alleged occurred in this district and that Defendants and/or agents of Defendants may be found in this district. Plaintiff and Defendants routinely engage in domestic and international financial transactions within and to this jurisdiction.

PARTIES

10. Plaintiff Amidax Trading Group (hereafter "Amidax") is a business based in the State of New Jersey. Amidax, a sole proprietorship, sells household cleaning products to customers throughout the world. Some of its customers are located in Israel, the United Arab Emirates, Qatar, Yemen, and other foreign countries.

11. Amidax is a customer of Defendant SWIFT[1] and uses a "SWIFT Code" – an account number that it uses to receive payments from its international business customers.

12. Amidax has held accounts at two different banks and used two different SWIFT Codes during the class period.

13. Amidax was receiving payments, via SWIFT, from its international customers prior to September 11, 2001 and in the weeks and months following that date continuing to the present.

14. Defendant SWIFT SCRL is an international corporation with its worldwide headquarters in La Hulpe, Belgium, and its principal North American place of business at 7 Times Square, 45th Floor, New York, New York 10036. It also operates a technology center in Manassas, Virginia.

15. Defendant SWIFT, Inc. is the name under which SWIFT SCRL's technology center in Manassas, Virginia is registered with the Secretary of State of the Commonwealth of Virginia.

16. Defendant SWIFT Pan-Americas Inc. is a wholly owned subsidiary of SWIFT SCRL and is the principal North American place of business of SWIFT SCRL. SWIFT Pan-

[1] Throughout the remainder of this Complaint, Defendants SWIFT SCRL, SWIFT Pan-Americas, Inc., and SWIFT, Inc. will be collectively referred to as "SWIFT" unless otherwise noted.

Americas Inc. is incorporated in the State of Delaware and its principal place of business is located at 7 Times Square, 45th Floor, New York, New York 10036.

17. Defendant John Snow was Secretary of the Treasury on September 11, 2001 and in the weeks and months following that date. Upon information and belief, Mr. Snow obtained the entire SWIFT database from Defendant SWIFT and also used an unconstitutionally overbroad administrative subpoena or subpoenas to request records of financial transactions from SWIFT.

18. Defendant Stuart Levey was an Under Secretary of the Treasury on September 11, 2001 and in the weeks and months following that date. Upon information and belief, Mr. Levey obtained the entire SWIFT database from Defendant SWIFT and also used an unconstitutionally overbroad administrative subpoena or subpoenas to request records of financial transactions from SWIFT.

19. Defendant George Tenet was Director of Operations of the Central Intelligence Agency on September 11, 2001 and in the weeks and months following that date. Upon information and belief, Mr. Tenet assisted or was otherwise complicit in the request and receipt of records of financial transactions from SWIFT.

20. Defendant Henry Paulson is the current Secretary of the Treasury. Upon information and belief, Mr. Paulson assisted or was otherwise complicit in the request and receipt of records of financial transactions from SWIFT.

21. Defendant Michael Hayden is the current Director of Operations of the Central Intelligence Agency. Upon information and belief, Mr. Hayden assisted or was otherwise complicit in the request and receipt of records of financial transactions from SWIFT.

22. Defendant George Bush is the President of the United States. Upon information and belief, President Bush ordered or approved the issuance of overbroad administrative subpoenas to SWIFT and accepted SWIFT's subsequent turnover of its entire database.

23. Defendant Richard Cheney is the Vice President of the United States. Upon information and belief, Vice President Cheney assisted or was otherwise complicit in the ordering or approval of the issuance of overbroad administrative subpoenas to SWIFT and the acceptance of SWIFT's subsequent turnover of its entire database.

24. Defendant United States Department of the Treasury is an agency of the United States Government located in Washington, D.C.

25. Defendant Central Intelligence Agency is an agency of the United States Government located in Langley, VA.

FACTUAL ALLEGATIONS RELATED TO ALL COUNTS

26. Upon information and belief, sometime after September 11, 2001, the Government Defendants made requests outside existing legal process for financial records from Defendant SWIFT.

27. Upon information and belief, sometime after September 11, 2001 SWIFT provided its entire database to the United States Government as part of the TFTP and acted in bad faith in so doing.

28. Upon information and belief, SWIFT disclosed Plaintiff's transactions when it provided its entire database to the United States Government as part of the TFTP.

29. Upon information and belief, SWIFT continues to disclose transactions to the United States Government as part of the TFTP.

30. Upon information and belief, the executive branch of the United States Government did not seek any judicial review in implementing the TFTP with SWIFT. No individual court-approved warrants or judicial subpoenas were sought or issued for the many millions of records in the database before it was disclosed.

31. According to U.S. Treasury Department Under Secretary Stuart Levey, at least one person has been removed from the operation for conducting a search considered inappropriate. (Treasury Department webcast of June 23, 2006 press conference, Ex. A, B).

32. Upon information and belief, transactions of Plaintiff and other class members were disclosed through the above-mentioned search or other searches the executive branch of the United States Government deemed or would deem inappropriate.

33. Upon information and belief, if an administrative subpoena or subpoenas were issued by the executive branch of the United States Government to SWIFT, SWIFT exceeded the scope of the subpoena or subpoenas in its response and acted in bad faith in so doing.

34. Upon information and belief, the Government Defendants acted in bad faith in accepting SWIFT's entire database.

35. On August 23, 2006, the Data Protection Commission for the German *Lander* of Schleswig-Holstein found that "The turn over of European citizens' financial data by SWIFT established in Belgium to United States authorities violates German and European data privacy law." ("Exhibit E").

36. On September 27, 2006, the Privacy Commission of Belgium found that "SWIFT should have complied with its obligations under the Belgian privacy law, amongst which the notification of the processing, the information, and the obligation to comply with the rules concerning personal data transfer to countries outside the EU" and that Swift was a "controller in

the processing of personal data via its SWIFTNet FIN service" and not "merely a processor, for example like a postal service."

37. On October 13, 2006, the Federal Data Protection and Information Commissioner of Switzerland concluded *inter alia* that "Swiss data protections laws must also have been infringed." ("Exhibit F").

38. On November 22, 2006, the Article 29 Working Party of the European Commission concluded *inter alia* that "Both SWIFT and instructing financial institutions share joint responsibility, although in different degrees, for the processing of personal data as 'data controllers'" and called upon SWIFT and the financial institutions "to take measures in order to remedy the currently illegal state of affairs without delay." ("Exhibit G").

39. At all times relevant, SWIFT was either itself a financial institution as that term is defined by 12 U.S.C. § 3414(d) and 31 U.S.C. §§ 5312(a) (1), (2) (R), (Y), and (Z) or acting as an agent of its member financial institutions.

40. At all times relevant, SWIFT acted as an instrument or agent of the United States Government.

41. SWIFT harmed the Plaintiff and the Nationwide Class he purports to represent when it illegally disclosed the transactions of the Plaintiff to the United States Government.

42. Upon information and belief, SWIFT did not inform the Plaintiff that it intended to disclose the Plaintiff's transactions to the United States Government. Had SWIFT done so, the Plaintiff would have had an informed opportunity to terminate his relationship with SWIFT.

43. Upon information and belief, SWIFT did not inform any of the other class members that it intended to disclose their transactions. Had it done so, the other class members would have had an informed opportunity to terminate their relationships with SWIFT.

CLASS ACTION ALLEGATIONS

44. Pursuant to Federal Rules of Civil Procedure, Rule 23 (a) and (b), Plaintiff Amidax brings this action on behalf of itself and a Nationwide Class of similarly situated persons defined as:

> All individuals and businesses in the United States that have used SWIFT to complete at least one financial transaction since September, 2001.

45. The Nationwide Class seeks certification of claims for declaratory relief, injunctive relief and damages pursuant to 12 U.S.C. § 3417 and 12 U.S.C. § 3418.

46. Plaintiff Amidax also brings the claims on behalf of the following New Jersey Subclass defined as:

> All individuals and businesses that are residents of the State of New Jersey and that have used SWIFT to complete at least one financial transaction since September, 2001.

47. The New Jersey Subclass seeks certification of claims for declaratory and injunctive relief, and for restitution.

48. Excluded from the Nationwide Class and New Jersey Subclass are the Defendants, the officers, directors, and employees of Defendants, and the legal representatives, heirs, successors, and assigns of Defendants.

49. This action is brought as a class action and may properly be so maintained pursuant to the provisions of the Federal Rules of Civil Procedure, Rule 23. Plaintiffs reserve the right to modify the Nationwide Class and the New Jersey Subclass definitions and the class period based on the results of discovery.

50. **Numerosity of the Nationwide Class and New Jersey Subclass:** Members of the Nationwide Class and New Jersey Subclass are so numerous that their individual joinder is

impracticable. The precise numbers and addresses of members of the Nationwide Class and New Jersey Subclass are unknown to the Plaintiffs. Plaintiffs estimate that the Nationwide Class and New Jersey Subclass consist of many thousands of members. The precise number of persons in both the Nationwide Class and New Jersey Subclass and their identities and addresses may be ascertained from Defendants' records.

51. There is a well-defined community of interest in the questions of law and fact involved affecting the members of the Nationwide Class and New Jersey Subclass. These common legal and factual questions include: (a) Whether Defendants have disclosed and/or accepted Nationwide Class members' financial records or other information in violation of the First and Fourth Amendments to the United States Constitution and Chapter 35 of Title 12, U.S.C., "The Right to Financial Privacy Act" (the "RFPA"); (b) Whether Defendants' disclosure and acceptance of New Jersey Subclass members' communications constitutes unfair, unlawful and/or fraudulent business practices in violation of New Jersey's Consumer Fraud Act[2] and numerous other state laws and statutes; (c) Whether Plaintiffs and New Jersey Subclass members are entitled to restitution, disgorgement of profits, or other equitable relief to remedy Defendants' unfair, unlawful and/or fraudulent business practices; (d) Whether Plaintiffs and class members are entitled to recover compensatory, statutory and punitive damages, whether as a result of Defendants' fraudulent, illegal and deceitful conduct, and/or otherwise; and (e) Whether Plaintiffs and class members are entitled to an award of reasonable attorneys' fees, pre-judgment interest, and costs of this suit.

52. **Typicality:** Plaintiff's claims are typical of the claims of the members of the Nationwide Class and New Jersey Subclass because Plaintiff has used SWIFT to complete many

---

[2] New Jersey Statutes Annotated, Title 56, Chapter 8

financial transactions since September 11, 2001. Plaintiffs and all members of the Nationwide Class and New Jersey Subclass have similarly suffered harm arising from Defendants' violations of law, as alleged herein.

53. **Adequacy:** Plaintiffs are adequate representatives of the Nationwide Class and New Jersey Subclass because their interests do not conflict with the interests of the members of the classes they seek to represent. Plaintiffs have retained counsel competent and experienced in complex class action litigation and intend to prosecute this action vigorously. Plaintiffs and their counsel will fairly and adequately protect the interests of the members of the Nationwide Class and New Jersey Subclass.

54. This suit may also be maintained as a class action pursuant to Federal Rules of Civil Procedure, Rule 23(b)(2) because Plaintiffs and both the Nationwide Class and New Jersey Subclass seek declaratory and injunctive relief, and all of the above factors of numerosity, common questions of fact and law, typicality and adequacy are present. Moreover, Defendants have acted on grounds generally applicable to Plaintiffs and both the Nationwide Class and New Jersey Subclass as a whole, thereby making declaratory and/or injunctive relief proper.

55. **Predominance and Superiority:** This suit may also be maintained as a class action under Federal Rules of Civil Procedure, Rule 23(b) (3) because questions of law and fact common to the Nationwide Class and New Jersey Subclass predominate over the questions affecting only individual members of the classes and a class action is superior to other available means for the fair and efficient adjudication of this dispute. The damages suffered by each individual class member may be relatively small, especially given the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. Furthermore, it would be virtually impossible for the class members, on an individual

basis, to obtain effective redress for the wrongs done to them. Moreover, even if class members themselves could afford such individual litigation, the court system could not. Individual litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties and the court system presented by the complex legal issue of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of a single adjudication, economy of scale and comprehensive supervision by a single court.

COUNT I

Violation of Plaintiffs' and Class Members' Rights Under the Fourth Amendment to the United States Constitution

56. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

57. On information and belief, the above-described acts of request, disclosure, and acceptance occurred without judicial review, individualized warrant or suspicion, probable cause, or other lawful authorization. On information and belief, the above-described acts of request, disclosure, and acceptance occurred wholly outside existing legal process.

58. By the acts alleged herein, Defendants Snow, Levey, United States Department of the Treasury, Bush, Central Intelligence Agency, Cheney, Tenet, Hayden, and Paulson violated Plaintiffs' and class members' reasonable expectations of privacy and denied Plaintiffs and class members their right to be free from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the Constitution of the United States.

59. By the acts alleged herein, Defendant SWIFT acted as an instrument or agent of the government, and thereby violated Plaintiffs' and class members' reasonable expectations of

privacy and denied Plaintiffs and class members their right to be free from unreasonable searches and seizures as guaranteed by the Fourth Amendment to the Constitution of the United States.

60. Wherefore, Plaintiffs and class members pray for this court to declare that Defendants haves violated their rights under the Fourth Amendment to the United States Constitution, and enjoin Defendants and their agents, successors and assigns from violating the Plaintiffs' and class members' rights under the Fourth Amendment to the United States Constitution.

COUNT II

Violation of Plaintiffs' and Class Members' Rights Under the First Amendment to the United States Constitution

61. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

62. Plaintiffs and class members have a reasonable expectation of privacy in their financial transactions transmitted, collected, and/or stored by SWIFT.

63. Plaintiffs and class members have a Constitutionally guaranteed right to free speech in the form of financial donations, contributions, or other expression of political, religious, or other personal beliefs through their financial transactions.

64. Plaintiffs and class members use SWIFT's services to complete financial transactions.

65. Upon information and belief, at all relevant times, Defendants failed to protect the First Amendment rights of the Plaintiffs and class members.

66. In performing the acts alleged herein, Defendant SWIFT had at all relevant times a primary or significant intent to assist or purpose of assisting the government in carrying out its "Terrorist Finance Tracking Program" (the "TFTP") and/or other government investigations, rather than to protect its own property rights.

67. By the acts alleged herein, the Government Defendants violated Plaintiffs' and class members' reasonable expectations of privacy and denied Plaintiffs and class members their rights to speak and receive speech privately under the First Amendment.

68. By the acts alleged herein, Defendant SWIFT acted as an instrument or agent of the government, and thereby violated Plaintiffs' and class members' reasonable expectations of privacy and denied Plaintiffs and class members their rights to speak and receive speech privately under the First Amendment.

69. By the acts alleged herein, Defendants' conduct proximately caused harm to Plaintiffs *and class members*.

70. On information and belief, Defendants' conduct was done intentionally, with deliberate indifference, or with reckless disregard of, Plaintiffs' and class members' Constitutional rights.

71. On information and belief, there is a strong likelihood that Defendants are now engaging in and will continue to engage in the above-described violations of Plaintiffs' and class members' Constitutional rights, either as principals or as agents of the Government, and that likelihood represents a credible threat of immediate future harm.

72. Wherefore, Plaintiffs and class members pray for this court to declare that Defendants have violated their rights under the First Amendment to the United States Constitution, and enjoin Defendants and their agents, successors, and assigns from violating the

Plaintiffs' and class members' rights under the First Amendment to the United States Constitution.

COUNT III

Disclosure and acceptance of financial records or information therein in violation of the United States Right to Financial Privacy Act, 12 U.S.C. 3401, *et seq.*

73. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

74. In relevant part, 12 U.S.C. §3402 provides that: Except as provided by section 3403(c) or (d), 3413, or 3414 of this title no Government authority may have access to or obtain copies of, or the information contained in the financial records of any customer from a financial institution unless the financial records are reasonably described and – (1) such customer has authorized such disclosure in accordance with section 3404 of this title; (2) such financial records are disclosed in response to an administrative subpoena or summons which meets the requirements of section 3405 of this title; (3) such financial records are disclosed in response to a search warrant which meets the requirements of section 3406 of this title; (4) such financial records are disclosed in response to a judicial subpoena which meets the requirements of section 3407 of this title; or (5) such financial records are disclosed in response to a formal written request which meets the requirements of section 3408 of this title.

75. Upon information and belief, Defendants requested, disclosed, and accepted information contained in customer financial records without reasonable description or any of the other five criteria enumerated above.

COUNT IV

Violation of State Wire Interception Statutes

76. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

77. Plaintiffs further state that Defendants have engaged and continue to engage in the unlawful interception of wire, oral, and/or electronic communications and the disclosure and/or divulgence and/or use of the contents of such communications.

78. The foregoing conduct violates the following state statutes:

a. Ala. Code §§ 13A-11-30, 13A-11-31 (2006)

b. Alaska Stat. § 42.20.310 (2005)

c. Ariz. Rev. Stat. Ann. § 13-3005 (2006)

d. Ark. Code Ann. § 5-60-120 (2005)

e. Cal. Penal Code § 630 *et seq.* (2006)

f. Colo. Rev. Stat. §§ 18-9-301, 18-9-303 (2006)

g. Conn. Gen. Stat. § 52-570d (2006)

h. Del. Code Ann. Tit. 11, § 2402 (2005)

i. D.C. Code §§ 23-541, 23-542 (2006)

j. Fla. Stat. §§ 934.01-03 (2005)

k. Ga. Code Ann. §§ 16-11-62 *et seq.* (2005)

l. Haw. Rev. Stat. § 803-42, 803-48 (2005)

m. Idaho Code Ann. § 18-6702 (2005)

n. 720 Ill. Comp. Stat. 5/14-1, -2 (2006)

o. Ind. Code § 35-33.5-1 *et seq.* (2005)

p. Iowa Code § 727.8 (2005)

q. Kan. Stat. Ann. §§ 21-4001, 21-4002 (2004)

r. Ky. Rev. Stat. Ann. §§ 526.010-.020 (2005)

s. La. Rev. Stat. Ann. § 15:1303 (2005)

t. Me. Rev. Stat. Ann. Tit. 15, §§ 709-710 (2006)

u. Md. Code Ann. Cts. & Jud. Proc. § 10-402 *et seq.*; § 10- 4A-4B *et seq.* (2006)

v. Mass. Gen. Laws ch. 272, § 99 (2006)

w. Mich. Comp. Laws § 750.539 *et seq.* (2006)

x. Minn. Stat. §§ 626A.01, .02 (2005)

y. Miss. Code Ann. § 41-29-501 *et seq.* (2006)

z. Mo. Rev. Stat. §§ 392.170, .350, 542.402, .418 (2006)

aa. Mont. Code Ann. § 45-8-213 (2006)

bb. Neb. Rev. Stat. § 86-290 (2006)

cc. Nev. Rev. Stat. 200.610-.620 (2006)

dd. N.H. Rev. Stat. Ann. §§ 570-A:1, -A:2 (2005)

ee. N.J. Stat. Ann. § 2A:156A-1 *et seq.* (2006)

ff. N.M. Stat. § 30-12-1 (2006)

gg. N.Y. Penal Law §§ 250.00, .05 (2006)

hh. N.C. Gen. Stat. § 15A-287 (2006)

ii. N.D. Cent. Code § 12.1-15-02 (2006)

jj. Ohio Rev. Code Ann. § 2933.51 *et seq.* (2006)

kk. Okla. Stat. tit. 13, § 176.1 *et seq.* (2006)

ll. Or. Rev. Stat. §§ 165.540, .543 (2006)

mm. 18 Pa. Cons. Stat. § 5701 *et seq.* (2005)

nn. R.I. Gen. Laws § 11-35-21 (2005)

oo. S.C. Code Ann. §§ 17-30-20, -30 (2005)

pp. S.D. Codified Laws §§ 23A-35A-1, 23A-35A-20 (2006)

qq. Tenn. Code Ann. § 39-13-601 (2006)

rr. Tex. Penal Code Ann. § 16.02 *et seq.*; Tex. Code Crim. Proc. art. 18.20 § 16(a) (2005)

ss. Utah Code Ann. § 77-23a-1 *et seq.* (2005)

tt. Va. Code Ann. §§ 19.2-61, -62 (2006)

uu. Wash. Rev. Code § 9.73.030 (2006)

vv. W. Va. Code § 62-1D-1 *et seq.* (2006)

ww. Wis. Stat. §§ 968.27, .31 (2005)

xx. Wyo. Stat. Ann. §§ 7-3-701, -702 (2005)

COUNT V

Violation of State Consumer Protection Statutes

79. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

80. Plaintiffs further state that Defendants violated and continue to violate state consumer protection statutes by requesting, divulging, and accepting records or other information pertaining to subscribers and customers to a governmental entity, without Class members' knowledge or consent.

81. The unfair and deceptive trade acts and practices of Defendants directly, foreseeably, and proximately caused damages and injury to Plaintiffs and the Class.

82. Defendants' actions and failure to act, including the false and misleading representations and omissions of material facts regarding the protection and use of Class members' private information, constitute unfair competition and/or unfair and/or deceptive acts or practices and/or false representations, in violation of the following state consumer protection statutes:

a. Ala. Code § 8-19-1 *et seq.*;

b. Alaska Stat. § 45.50.531(a);

c. Ariz. Rev. Stat. § 44-1522 *et seq.*;

d. Ark. Code § 4-88-101 *et seq.*;

e. Cal. Bus. & Prof. Code § 17200 *et seq.*;

f. Colo. Rev. Stat. § 6-1-105 *et seq.*;

g. Conn. Gen. Stat. § 42-110b *et seq.*;

h. *6* Del. Code § 2511 *et seq.*;

i. D.C. Code Ann. § 28-3901 *et seq.*;

j. Fla. Stat. § 501.201 *et seq.*;

k. Ga. Stat. § 10-1-392 *et seq.*;

l. Haw. Rev. Stat. § 480 *et seq.*;

m. Idaho Code § 48-601 *et seq.*;

n. 815 Ill. Comp. Stat. § 505.1 *et seq.*;

o. Ind. Code § 24-5-0.5 *et seq.*;

p. Iowa Code § 714.16 *et seq.*;

q. Kan. Stat. Ann. § 50-623 *et seq.*;

r. Ky. Rev. Stat. § 367.1 10 *et seq.*;

s. La. Rev. Stat. § 51:1401 *et seq.*;

t. 5 Me. Rev. Stat. Ann. § 207 *et seq.*;

u. Massachusetts General Laws Ch. 93A *et seq.*;

v. Md. Com. Law Code § 13-101 et seq.

w. Mich. Stat. § 445.901 *et seq.*;

x. Minn. Stat. § 8.31 *et seq.*;

y. Miss. Code Ann. § 75-24-1 *et seq.*;

z. Mo. Ann. Stat. § 407.010 *et seq.*;

aa. Mont. Code § 30-14-101 *et seq.*;

bb. Neb. Rev. Stat. § 59-1601 *et seq.*;

cc. Nev. Rev. Stat. § 598.0903 *et seq.*;

dd. N.H. Rev. Stat. § 358-A:1 *et seq.*;

ee. N.J. Rev. Stat. § 56:8-1 *et seq.*;

ff. N.M. Stat. § 57-12-1 *et seq.*;

gg. N.Y. Gen. Bus. Law § 349 *et seq.*;

hh. N.C. Gen. Stat. §§ 75-1.1 *et seq.*;

ii. N.D. Cent. Code § 51-15-01 *et seq.*;

jj. Ohio Rev. Stat. § 1345.01 *et seq.*;

kk. Okla. Stat. 15 § 751 *et seq.*;

ll. Or. Rev. Stat. § 646.605 *et seq.*;

mm. 73 Pa. Stat. § 201-1 *et seq.*;

nn. R.I. Gen. Laws § 6-13.1-1 *et seq.*;

oo. S.C. Code Laws § 39-5-10 *et seq.*;

pp. S.D. Code Laws § 37-241 *et seq.*;

qq. Tenn. Code Ann. § 47-18-101 *et seq.*;

rr. Tex. Bus. & Com. Code § 17.41 *et seq.*;

ss. Utah Code § 13-11-1 *et seq.*;

tt. 9 Vt. Stat. § 2451 *et seq.*;

uu. Va. Code § 59.1-196 *et seq.*;

vv. Wash. Rev. Code § 19.86.010 *et seq.*;

ww. W. Va. Code § 46A-6-101 *et seq.*;

xx. Wis. Stat. § 100.18 *et seq.*; and

yy. Wyo. Stat. Ann. § 40-12-101 et seq.

83. This injury is of the type the state consumer protection and deceptive practices statutes were designed to prevent and directly results from Defendants' unlawful conduct.

COUNT VI

Violation of State Constitutions

84. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

85. Plaintiffs further state that Defendants violated and continue to violate the Constitutions of the nation's member states by requesting, divulging, and accepting records or other information pertaining to subscribers and customers to a governmental entity, without Class members' knowledge or consent.

COUNT VII

Breach of Contract

86. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

87. At all times relevant herein, Defendant SWIFT agreed to provide Plaintiffs with services either directly or in a third party beneficiary capacity.

88. At all times relevant herein, Defendant SWIFT impliedly and expressly promised to protect the privacy and confidentiality of their customers' information, identity, records, use details, and communications, and to abide by federal and state law.

89. Defendant SWIFT by its conduct as alleged breached its contract with the Plaintiff and Class Members. Defendant SWIFT has also by its conduct as alleged breached the implied covenant of good faith and fair dealing[3].

90. As a result of Defendant SWIFT's breach of contractual duties owed to the Plaintiffs and Class members, Defendant SWIFT is liable for damages including, but not limited to nominal and consequential damages.

COUNT VIII

Breach of Warranty

91. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

92. At all times relevant herein, Defendant SWIFT agreed to provide Plaintiffs and Class Members with services either directly or as third party beneficiaries.

93. At all times relevant herein, Defendant SWIFT impliedly and expressly warranted or otherwise represented to Plaintiffs and Class Members that Defendants would safeguard, protect, and maintain the privacy and confidentiality of their customers' information, identity, records, and communications, and to abide by all applicable law.

94. Plaintiffs and Class members relied upon these express and implied warranties and representations in their dealings with Defendant SWIFT.

95. At all times relevant, Defendant SWIFT by its conduct as alleged, breached those warranties and representations.

[3] Plaintiffs preserve such claims with respect to states in which breach of the implied covenant of good faith and fair dealing is pled separately.

96. As a direct and proximate result of Defendant SWIFT's breaches of warranty as detailed herein, Plaintiffs and Class Members have suffered damages including, but not limited to, nominal and consequential damages.

PRAYER FOR RELIEF

WHEREFORE, the Plaintiff for itself and all others similarly situated respectfully requests that the Court:

A. Declare that Defendants' request, disclosure, and acceptance of financial records as alleged herein violates applicable law including without limitation:

(i) The Fourth Amendment to the United States Constitution; and

(ii) The First Amendment to the United States Constitution; and

(ii) The Right to Financial Privacy Act; 12 U.S.C. § 3401, *et seq.*; and

(iv) The state laws, statutes, and Constitutions outlined above.

B. Award equitable relief, including without limitation, a preliminary and permanent injunction prohibiting Defendants' continued or future illegal request, disclosure, and acceptance of financial records:

(i) Pursuant to the First and Fourth Amendments to the United States Constitution and 12 U.S.C. §3417, as to the Plaintiffs and the Nationwide Class.

(ii) Pursuant to the New Jersey Consumer Fraud Act as to the Plaintiffs and the New Jersey Class.

C. Award statutory damages to the extent permitted by law to each Plaintiff and class member in the sum of:

(i) $100 per day for each day of violation of 12 U.S.C. §3402, pursuant to 12 U.S.C. §3417; and

D. Award punitive damages to the extent permitted by law to each Plaintiff and class member, including without limitation:

(i) An appropriate sum pursuant to 12 U.S.C. § 3417.

E. Award to Plaintiffs attorneys' fees and other costs of suit to the extent permitted by law pursuant to 12 U.S.C. §3417.

F. Grant such other and further relief as the Court deems just and proper.

Plaintiffs respectfully move for leave to amend should the Court identify any defects in this Complaint.

JURY DEMAND

Plaintiffs hereby request a jury trial for all issues triable by jury including, but not limited to, those issues and claims set forth in any amended complaint or consolidated action.

DATED: June 23, 2008

AMIDAX TRADING GROUP, on behalf of itself and all others similarly situated.

By: _____

Steven E. Schwarz, Esq.
THE LAW OFFICES OF STEVEN E. SCHWARZ, ESQ., LLC
2461 W. Foster Ave., #1W
Chicago, IL 60625
Telephone: 773/837-6134
stevenschwarz23@yahoo.com

MAYER LAW GROUP, LLC
CARL J. MAYER, ESQ.
66 Witherspoon Street, Suite 414
Princeton, NJ 08542
Telephone: 609/921-8025
Facsimile: 609/921-6964

Attorneys for Plaintiff

Bruce I. Afran

BRUCE I. AFRAN, ESQ. BA-8583
10 Braeburn Drive
Princeton, NJ 08540
609/924-2075

EXHIBIT A

** PLACEHOLDER FOR DVD FILED

IN PLAIN YELLOW ENVELOPE AS "EXHIBIT A" **

EXHIBIT B

UNITED STATES
DEPARTMENT OF THE TREASURY

OFFICE OF PUBLIC AFFAIRS

search SEARCH

News
Direct Links
Key Topics
Press Room
About Treasury
Offices
- Domestic Finance
- Economic Policy
- General Counsel
- International Affairs
- Management
- Public Affairs
  - E-mail Subscription Service
  - Media Advisories
  - Treasury Bureaus' Public Affairs Sites
  - Federal Public Affairs Sites
- Tax Policy
- Terrorism and Financial Intelligence
- Treasurer

Bureaus
Education
Site Policies and Notices

VIDEO WEBCAST CENTER

< BACK

WEBCAST LIBRARY
2008 | 2007 | **2006** | 2005 | 2004 | 2003 | 2002

November 1, 2006
Quarterly Refunding Webcast

Deputy Assistant Secretary James Clouse

View in Real Player Format
View in Windows Media

For the hearing impaired, view with captioning:
View in Real Player format
View in Windows Media

September 13, 2006
Speech on the International Economy

Treasury Secretary Henry M. Paulson, Jr.

View in Real Player Format
View in Windows Media

For the hearing impaired, view with captioning:
View in Real Player format
View in Windows Media

August 02, 2006
August Quarterly Refunding

Assistant Secretary for Financial Institutions Emil Henry
Deputy Assistant Secretary for Federal Finance James Clouse
Debt Management Director Jeff Huther

View in Real Player Format
View in Windows Media

For the hearing impaired, view with captioning:
View in Real Player format
View in Windows Media

July 10, 2006
Swearing-In Ceremony for Incoming Treasury Secretary for Henry M. Paulson, Jr.

View in Real Player Format

View in Windows Media

For the hearing impaired, view with captioning:
View in Real Player format
View in Windows Media

June 23, 2006
Terrorist Finance Tracking Program

Treasury Secretary John W. Snow
Under Secretary for Terrorism and Financial Intelligence Stuart Levey

View in Real Player Format
View in Windows Media

For the hearing impaired, view with captioning:
View in Real Player format
View in Windows Media

MAY 16, 2006
Economic Media Briefing

Secretary John W. Snow

View in Real Player Format
View in Windows Media

For the hearing impaired, view with captioning:
View in Real Player format
View in Windows Media

MAY 10, 2006
Semiannual Report on International Economic and Exchange Rate Policies

Secretary John W. Snow

View in Real Player Format
View in Windows Media Format

For the hearing impaired, view with captioning:
View in Real Player format
View in Windows Media

MAY 3, 2006
May Quarterly Refunding

Assistant Secretary for Financial Institutions Emil Henry
Deputy Assistant Secretary for Federal Finance James Clouse
Debt Management Director Jeff Huther

View in Real Player format:
For high speed internet users (150k)
For dialup modem users (28k)

View in Windows Media format:
For all users

For the hearing impaired, view with closed captioning:
Real Player
Windows Media

MAY 1, 2006
2006 Social Security and Medicare Trustees Report Press Conference

Secretary of Treasury and Managing Trustee John W. Snow
Secretary of Labor and Trustee Elaine L. Chao
Secretary of Health and Human Service and Trustee Michael Leavitt
Commissioner of Social Security and Trustee Jo Anne Barnhart
Public Trustee John Palmer and Public Trustee Thomas Saving

View in Real Player format:
For high speed internet users (150k)
For dialup modem users (28k)

View in Windows Media format:
For all users

For the hearing impaired, view with closed captioning:
Real Player
Windows Media

APRIL 19, 2006
Pre-G7 Press Briefing
Under Secretary for International Affairs Timothy Adams

View in Real Player format:
For high speed internet users (150k)
For dialup modems (28k)

View in Windows Media format:
For high speed internet users (150k)
For dialup modem users (28k)

For the hearing impaired, view with closed captioning turned on in the player:
Real Player
Windows Media

FEBRUARY 6, 2006
Blue Book Briefing
Assistant Secretary for Public Affairs Tony Fratto
Deputy Assistant Secretary for Tax Analysis Bob Carroll
Deputy Assistant Secretary for Regulatory Affairs Eric Solomon

View in Real Player format:
For high speed internet users (150k)
For dialup modems (28k)

View in Windows Media format:
For all users

For the hearing impaired, view with closed captioning turned on in the player:
Real Player
Windows Media

FEBRUARY 1, 2006
February Quarterly Refunding
Under Secretary for Domestic Finance Randal K. Quarles
Office of Debt Management Director Jeff Huther
November Quarterly Refunding Press Briefing

View in Real Player format:
For high speed internet users (150k)

For dialup modems (28k)

View in Windows Media format:
For all users

For the hearing impaired, view with closed captioning turned on in the player:
Real Player
Windows Media

JANUARY 26, 2006
Identity Theft: Outsmarting the Crooks

View in Real Player format:
For high speed internet users (150k)
For dialup modems (28k)

View in Windows Media format:
For all users

For the hearing impaired, view with closed captioning turned on in the player:
Real Player
Windows Media

EXHIBIT C

The New York Times
nytimes.com

June 23, 2006

BANK DATA SIFTED IN SECRET BY U.S. TO BLOCK TERROR

By ERIC LICHTBLAU AND JAMES RISEN; BARCLAY WALSH CONTRIBUTED REPORTING FOR THIS ARTICLE.

Under a secret Bush administration program initiated weeks after the Sept. 11 attacks, counterterrorism officials have gained access to financial records from a vast international database and examined banking transactions involving thousands of Americans and others in the United States, according to government and industry officials.

The program is limited, government officials say, to tracing transactions of people suspected of having ties to Al Qaeda by reviewing records from the nerve center of the global banking industry, a Belgian cooperative that routes about $6 trillion daily between banks, brokerages, stock exchanges and other institutions. The records mostly involve wire transfers and other methods of moving money overseas and into and out of the United States. Most routine financial transactions confined to this country are not in the database.

Viewed by the Bush administration as a vital tool, the program has played a hidden role in domestic and foreign terrorism investigations since 2001 and helped in the capture of the most wanted Qaeda figure in Southeast Asia, the officials said.

The program, run out of the Central Intelligence Agency and overseen by the Treasury Department, "has provided us with a unique and powerful window into the operations of terrorist networks and is, without doubt, a legal and proper use of our authorities," Stuart Levey, an under secretary at the Treasury Department, said in an interview on Thursday.

The program is grounded in part on the president's emergency economic powers, Mr. Levey said, and multiple safeguards have been imposed to protect against any unwarranted searches of Americans' records.

The program, however, is a significant departure from typical practice in how the government acquires Americans' financial records. Treasury officials did not seek individual court-approved warrants or subpoenas to examine specific transactions, instead relying on broad administrative subpoenas for millions of records from the cooperative, known as Swift.

That access to large amounts of confidential data was highly unusual, several officials said, and stirred concerns inside the administration about legal and privacy issues.

"The capability here is awesome or, depending on where you're sitting, troubling," said one former senior counterterrorism official who considers the program valuable. While tight controls are in place, the official added, "the potential for abuse is enormous."

The program is separate from the National Security Agency's efforts to eavesdrop without warrants and collect domestic phone records, operations that have provoked fierce public debate and spurred

lawsuits against the government and telecommunications companies.

But all the programs grew out of the Bush administration's desire to exploit technological tools to prevent another terrorist strike, and all reflect attempts to break down longstanding legal or institutional barriers to the government's access to private information about Americans and others inside the United States.

Officials described the Swift program as the biggest and most far-reaching of several secret efforts to trace terrorist financing. Much more limited agreements with other companies have provided access to A.T.M. transactions, credit card purchases and Western Union wire payments, the officials said.

Nearly 20 current and former government officials and industry executives discussed aspects of the Swift operation with The New York Times on condition of anonymity because the program remains classified. Some of those officials expressed reservations about the program, saying that what they viewed as an urgent, temporary measure had become permanent nearly five years later without specific Congressional approval or formal authorization.

Data from the Brussels-based banking consortium, formally known as the Society for Worldwide Interbank Financial Telecommunication, has allowed officials from the C.I.A., the Federal Bureau of Investigation and other agencies to examine "tens of thousands" of financial transactions, Mr. Levey said.

While many of those transactions have occurred entirely on foreign soil, officials have also been keenly interested in international transfers of money by individuals, businesses, charities and other groups under suspicion inside the United States, officials said. A small fraction of Swift's records involve transactions entirely within this country, but Treasury officials said they were uncertain whether any had been examined.

Swift executives have been uneasy at times about their secret role, the government and industry officials said. By 2003, the executives told American officials they were considering pulling out of the arrangement, which began as an emergency response to the Sept. 11 attacks, the officials said. Worried about potential legal liability, the Swift executives agreed to continue providing the data only after top officials, including Alan Greenspan, then chairman of the Federal Reserve, intervened. At that time, new controls were introduced.

Among the safeguards, government officials said, is an outside auditing firm that verifies that the data searches are based on intelligence leads about suspected terrorists. "We are not on a fishing expedition," Mr. Levey said. "We're not just turning on a vacuum cleaner and sucking in all the information that we can."

Swift and Treasury officials said they were aware of no abuses. But Mr. Levey, the Treasury official, said one person had been removed from the operation for conducting a search considered inappropriate.

Treasury officials said Swift was exempt from American laws restricting government access to private financial records because the cooperative was considered a messaging service, not a bank or financial institution.

But at the outset of the operation, Treasury and Justice Department lawyers debated whether the

program had to comply with such laws before concluding that it did not, people with knowledge of the debate said. Several outside banking experts, however, say that financial privacy laws are murky and sometimes contradictory and that the program raises difficult legal and public policy questions.

The Bush administration has made no secret of its campaign to disrupt terrorist financing, and President Bush, Treasury officials and others have spoken publicly about those efforts. Administration officials, however, asked The New York Times not to publish this article, saying that disclosure of the Swift program could jeopardize its effectiveness. They also enlisted several current and former officials, both Democrat and Republican, to vouch for its value.

Bill Keller, the newspaper's executive editor, said: "We have listened closely to the administration's arguments for withholding this information, and given them the most serious and respectful consideration. We remain convinced that the administration's extraordinary access to this vast repository of international financial data, however carefully targeted use of it may be, is a matter of public interest."

Mr. Levey agreed to discuss the classified operation after the Times editors told him of the newspaper's decision.

On Thursday evening, Dana Perino, deputy White House press secretary, said: "Since immediately following 9/11, the American government has taken every legal measure to prevent another attack on our country. One of the most important tools in the fight against terror is our ability to choke off funds for the terrorists."

She added: "We know the terrorists pay attention to our strategy to fight them, and now have another piece of the puzzle of how we are fighting them. We also know they adapt their methods, which increases the challenge to our intelligence and law enforcement officials."

Referring to the disclosure by The New York Times last December of the National Security Agency's eavesdropping program, she said, "The president is concerned that once again The New York Times has chosen to expose a classified program that is working to protect our citizens."

Swift declined to discuss details of the program but defended its role in written responses to questions. "Swift has fully complied with all applicable laws," the consortium said. The organization said it insisted that the data be used only for terrorism investigations and had narrowed the scope of the information provided to American officials over time.

A Crucial Gatekeeper

Swift's database provides a rich hunting ground for government investigators. Swift is a crucial gatekeeper, providing electronic instructions on how to transfer money among 7,800 financial institutions worldwide. The cooperative is owned by more than 2,200 organizations, and virtually every major commercial bank, as well as brokerage houses, fund managers and stock exchanges, uses its services. Swift routes more than 11 million transactions each day, most of them across borders.

The cooperative's message traffic allows investigators, for example, to track money from the Saudi bank account of a suspected terrorist to a mosque in New York. Starting with tips from intelligence reports about specific targets, agents search the database in what one official described as a "24-7" operation. Customers' names, bank account numbers and other identifying information can be

retrieved, the officials said.

The data does not allow the government to track routine financial activity, like A.T.M. withdrawals, confined to this country, or to see bank balances, Treasury officials said. And the information is not provided in real time -- Swift generally turns it over several weeks later. Because of privacy concerns and the potential for abuse, the government sought the data only for terrorism investigations and prohibited its use for tax fraud, drug trafficking or other inquiries, the officials said.

The Treasury Department was charged by President Bush, in a September 2001 executive order, with taking the lead role in efforts to disrupt terrorist financing. Mr. Bush has been briefed on the program and Vice President Dick Cheney has attended C.I.A. demonstrations, the officials said. The National Security Agency has provided some technical assistance.

While the banking program is a closely held secret, administration officials have held classified briefings for some members of Congress and the Sept. 11 commission, the officials said. More lawmakers were briefed in recent weeks, after the administration learned The Times was making inquiries for this article.

Swift's 25-member board of directors, made up of representatives from financial institutions around the world, was previously told of the program. The Group of 10's central banks, in major industrialized countries, which oversee Swift, were also informed. It is not clear if other network participants know that American intelligence officials can examine their message traffic.

Because Swift is based overseas and has offices in the United States, it is governed by European and American laws. Several international regulations and policies impose privacy restrictions on companies that are generally regarded as more stringent than those in this country. United States law establishes some protections for the privacy of Americans' financial data, but they are not ironclad. A 1978 measure, the Right to Financial Privacy Act, has a limited scope and a number of exceptions, and its role in national security cases remains largely untested.

Several people familiar with the Swift program said they believed that they were exploiting a "gray area" in the law and that a case could be made for restricting the government's access to the records on Fourth Amendment and statutory grounds. They also worried about the impact on Swift if the program were disclosed.

"There was always concern about this program," a former official said.

One person involved in the Swift program estimated that analysts had reviewed international transfers involving "many thousands" of people or groups in the United States. Two other officials placed the figure in the thousands. Mr. Levey said he could not estimate the number.

The Swift data has provided clues to money trails and ties between possible terrorists and groups financing them, the officials said. In some instances, they said, the program has pointed them to new suspects, while in others it has buttressed cases already under investigation.

Among the successes was the capture of a Qaeda operative, Riduan Isamuddin, better known as Hambali, believed to be the mastermind of the 2002 bombing of a Bali resort, several officials said. The Swift data identified a previously unknown figure in Southeast Asia who had financial dealings with a person suspected of being a member of Al Qaeda; that link helped locate Hambali in Thailand

in 2003, they said.

In the United States, the program has provided financial data in investigations into possible domestic terrorist cells as well as inquiries of Islamic charities with suspected of having links to extremists, the officials said.

The data also helped identify a Brooklyn man who was convicted on terrorism-related charges last year, the officials said. The man, Uzair Paracha, who worked at a New York import business, aided a Qaeda operative in Pakistan by agreeing to launder $200,000 through a Karachi bank, prosecutors said.

In terrorism prosecutions, intelligence officials have been careful to "sanitize," or hide the origins of evidence collected through the program to keep it secret, officials said.

The Bush administration has pursued steps that may provide some enhanced legal standing for the Swift program. In late 2004, Congress authorized the Treasury Department to develop regulations requiring American banks to turn over records of international wire transfers. Officials say a preliminary version of those rules may be ready soon. One official described the regulations as an attempt to "formalize" access to the kind of information secretly provided by Swift, though other officials said the initiative was unrelated to the program.

The Scramble for New Tools

Like other counterterrorism measures carried out by the Bush administration, the Swift program began in the hectic days after the Sept. 11 attacks, as officials scrambled to identify new tools to head off further strikes.

One priority was to cut off the flow of money to Al Qaeda. The 9/11 hijackers had helped finance their plot by moving money through banks. Nine of the hijackers, for instance, funneled money from Europe and the Middle East to SunTrust bank accounts in Florida. Some of the $130,000 they received was wired by people overseas with known links to Al Qaeda.

Financial company executives, many of whom had lost friends at the World Trade Center, were eager to help federal officials trace terrorist money. "They saw 9/11 not just as an attack on the United States, but on the financial industry as a whole," said one former government official.

Quietly, counterterrorism officials sought to expand the information they were getting from financial institutions. Treasury officials, for instance, spoke with credit card companies about devising an alert if someone tried to buy fertilizer and timing devices that could be used for a bomb, but they were told the idea was not logistically possible, a lawyer in the discussions said.

The F.B.I. began acquiring financial records from Western Union and its parent company, the First Data Corporation. The programs were alluded to in Congressional testimony by the F.B.I. in 2003 and described in more detail in a book released this week, "The One Percent Doctrine," by Ron Suskind. Using what officials described as individual, narrowly framed subpoenas and warrants, the F.B.I. has obtained records from First Data, which processes credit and debit card transactions, to track financial activity and try to locate suspects.

Similar subpoenas for the Western Union data allowed the F.B.I. to trace wire transfers, mainly outside the United States, and to help Israel disrupt about a half-dozen possible terrorist plots there by

unraveling the financing, an official said.

The idea for the Swift program, several officials recalled, grew out of a suggestion by a Wall Street executive, who told a senior Bush administration official about Swift's database. Few government officials knew much about the consortium, which is led by a Brooklyn native, Leonard H. Schrank, but they quickly discovered it offered unparalleled access to international transactions. Swift, a former government official said, was "the mother lode, the Rosetta stone" for financial data.

Intelligence officials were so eager to use the Swift data that they discussed having the C.I.A. covertly gain access to the system, several officials involved in the talks said. But Treasury officials resisted, the officials said, and favored going to Swift directly.

At the same time, lawyers in the Treasury Department and the Justice Department were considering possible legal obstacles to the arrangement, the officials said.

In 1976, the Supreme Court ruled that Americans had no constitutional right to privacy for their records held by banks or other financial institutions. In response, Congress passed the Right to Financial Privacy Act two years later, restricting government access to Americans' banking records. In considering the Swift program, some government lawyers were particularly concerned about whether the law prohibited officials from gaining access to records without a warrant or subpoena based on some level of suspicion about each target.

For many years, law enforcement officials have relied on grand-jury subpoenas or court-approved warrants for such financial data. Since 9/11, the F.B.I. has turned more frequently to an administrative subpoena, known as a national security letter, to demand such records.

After an initial debate, Treasury Department lawyers, consulting with the Justice Department, concluded that the privacy laws applied to banks, not to a banking cooperative like Swift. They also said the law protected individual customers and small companies, not the major institutions that route money through Swift on behalf of their customers.

Other state, federal and international regulations place different and sometimes conflicting restrictions on the government's access to financial records. Some put greater burdens on the company disclosing the information than on the government officials demanding it.

Among their considerations, American officials saw Swift as a willing partner in the operation. But Swift said its participation was never voluntary. "Swift has made clear that it could provide data only in response to a valid subpoena," according to its written statement.

Indeed, the cooperative's executives voiced early concerns about legal and corporate liability, officials said, and the Treasury Department's Office of Foreign Asset Control began issuing broad subpoenas for the cooperative's records related to terrorism. One official said the subpoenas were intended to give Swift some legal protection.

Underlying the government's legal analysis was the International Emergency Economic Powers Act, which Mr. Bush invoked after the 9/11 attacks. The law gives the president what legal experts say is broad authority to "investigate, regulate or prohibit" foreign transactions in responding to "an unusual and extraordinary threat."

But L. Richard Fischer, a Washington lawyer who wrote a book on banking privacy and is regarded as a leading expert in the field, said he was troubled that the Treasury Department would use broad subpoenas to demand large volumes of financial records for analysis. Such a program, he said, appears to do an end run around bank-privacy laws that generally require the government to show that the records of a particular person or group are relevant to an investigation.

"There has to be some due process," Mr. Fischer said. "At an absolute minimum, it strikes me as inappropriate."

Several former officials said they had lingering concerns about the legal underpinnings of the Swift operation. The program "arguably complies with the letter of the law, if not the spirit," one official said.

Another official said: "This was creative stuff. Nothing was clear cut, because we had never gone after information this way before."

Treasury officials said they considered the government's authority to subpoena the Swift records to be clear. "People do not have a privacy interest in their international wire transactions," Mr. Levey, the Treasury under secretary, said.

Tighter Controls Sought

Within weeks of 9/11, Swift began turning over records that allowed American analysts to look for evidence of terrorist financing. Initially, there appear to have been few formal limits on the searches.

"At first, they got everything -- the entire Swift database," one person close to the operation said.

Intelligence officials paid particular attention to transfers to or from Saudi Arabia and the United Arab Emirates because most of the 9/11 hijackers were from those countries.

The volume of data, particularly at the outset, was often overwhelming, officials said. "We were turning on every spigot we could find and seeing what water would come out," one former administration official said. "Sometimes there were hits, but a lot of times there weren't."

Officials realized the potential for abuse, and narrowed the program's targets and put in more safeguards. Among them were the auditing firm, an electronic record of every search and a requirement that analysts involved in the operation document the intelligence that justified each data search. Mr. Levey said the program was used only to examine records of individuals or entities, not for broader data searches.

Despite the controls, Swift executives became increasingly worried about their secret involvement with the American government, the officials said. By 2003, the cooperative's officials were discussing pulling out because of their concerns about legal and financial risks if the program were revealed, one government official said.

"How long can this go on?" a Swift executive asked, according to the official.

Even some American officials began to question the open-ended arrangement. "I thought there was a limited shelf life and that this was going to go away," the former senior official said.

In 2003, administration officials asked Swift executives and some board members to come to Washington. They met with Mr. Greenspan, Robert S. Mueller III, the F.B.I. director, and Treasury officials, among others, in what one official described as "a full-court press." Aides to Mr. Greenspan and Mr. Mueller declined to comment on the meetings.

The executives agreed to continue supplying records after the Americans pledged to impose tighter controls. Swift representatives would be stationed alongside intelligence officials and could block any searches considered inappropriate, several officials said.

The procedural change provoked some opposition at the C.I.A. because "the agency was chomping at the bit to have unfettered access to the information," a senior counterterrorism official said. But the Treasury Department saw it as a necessary compromise, the official said, to "save the program."

EXHIBIT D

The New York Times

June 24, 2006

Cheney Assails Press on Report on Bank Data

By SHERYL GAY STOLBERG and ERIC LICHTBLAU

WASHINGTON, June 23 — Vice President Dick Cheney on Friday vigorously defended a secret program that examines banking records of Americans and others in a vast international database, and harshly criticized the news media for disclosing an operation he said was legal and "absolutely essential" to fighting terrorism.

"What I find most disturbing about these stories is the fact that some of the news media take it upon themselves to disclose vital national security programs, thereby making it more difficult for us to prevent future attacks against the American people," Mr. Cheney said, in impromptu remarks at a fund-raising luncheon for a Republican Congressional candidate in Chicago. "That offends me."

The financial tracking program was disclosed Thursday by The New York Times and other news organizations. American officials had expressed concerns that the Brussels banking consortium that provides access to the database might withdraw from the program if its role were disclosed, particularly in light of anti-American sentiment in some parts of Europe.

But the consortium, the Society for Worldwide Interbank Financial Telecommunication, or Swift, published a statement on its Web site on Friday, saying its executives "have done their utmost to get the right balance in fulfilling their obligations to the authorities in a manner protective of the interests of the company and its members."

A representative for the cooperative, speaking on condition of anonymity because he was not allowed to talk about its internal discussions, said that he knew of no discussions about withdrawing, adding that the group was "very resolute" in its commitment to the financial tracking operation.

The program, run out of the Central Intelligence Agency and overseen by the Treasury Department, has allowed counterterrorism authorities to gain access to millions of records of transactions routed through Swift from individual banks and financial institutions around the world. The data is obtained using broad administrative subpoenas, not court warrants.

Investigators have used the data to do "at least tens of thousands, maybe hundreds of thousands of searches" of people and institutions suspected of having ties to terrorists, Stuart Levey, an under secretary at the Treasury Department, told reporters at a briefing on Friday. Officials say the program has proven valuable in a number of foreign and domestic terrorism investigations, and led to the 2003 capture of the most wanted Qaeda fugitive in Southeast Asia, known as Hambali.

News accounts of the program appeared just as President Bush returned from a two-day trip to Europe, where he met in Vienna with leaders of the European Union. Neither that organization nor any of its member

states commented Friday, but one advocate for civil liberties in London said the program could create new tensions in Europe just as Mr. Bush was trying to smooth trans-Atlantic relations.

"Our data has been effectively hijacked by the U.S. under cover of secret agreements and entirely undisclosed terms," said the civil liberties advocate, Simon Davies, the director of Privacy International, a London-based organization focused on the intrusion on privacy by governments and businesses. "There will be a snapping point, and this may be it."

Initial reaction from global banks was muted, with one executive saying that while the privacy of information was a contentious issue within the industry, the Swift operation had so far generated few complaints.

In Washington on Friday, privacy groups and civil liberties advocates were critical of the program, as were some Democrats and one prominent Republican on Capitol Hill.

The executive director of the American Civil Liberties Union, Anthony D. Romero, condemned the program, calling it "another example of the Bush administration's abuse of power."

Lauren Weinstein, the head of the California-based Privacy Forum, an online discussion group, raised concerns about lack of independent review of the operation. "Oversight is the difference between something being reasonable and something being abuse," he said.

Senator Arlen Specter, Republican of Pennsylvania and chairman of the Senate Judiciary Committee, said he had sent letters on Friday to both Treasury Secretary John W. Snow and Attorney General Alberto R. Gonzales on the issue. While he declined to release the letters, he said he was concerned about the legal authority for the operation.

Mr. Specter has been at odds with the administration over another previously secret counterterrorism operation, the National Security Agency's domestic eavesdropping program. The senator said he was particularly troubled that the administration had expanded its Congressional briefings on the financial tracking program in recent weeks after having learned that The New York Times was making inquiries.

"Why does it take a newspaper investigation to get them to comply with the law?" the senator asked. "That's a big, important point."

In explaining the program, Mr. Levey, the Treasury under secretary who oversees the program, said in an interview earlier in the week that "people do not have a privacy interest in their international wire transactions." But Mr. Specter was skeptical.

"I'm not surprised that a Treasury official would take that position, but I'm not so sure he's right," the senator said. "I don't think it's an open-and-shut question."

Representative Edward J. Markey, the Massachusetts Democrat who has made privacy a signature issue, said, "I am very concerned that the Bush administration may be once again violating the constitutional rights of innocent Americans as part of another secret program created in the aftermath of the Sept. 11 attacks."

But Mr. Cheney was emphatic on Friday in arguing the program is necessary, and predicted that the Bush

administration might be criticized over it in much the same way that critics have assailed the National Security Agency eavesdropping, which has been done without warrants.

"The fact of the matter is that these are good, solid, sound programs," the vice president said at the fund-raiser in Chicago for David McSweeney, a Republican who is running against Representative Melissa Bean, a freshman Democrat.

"They are conducted in accordance with the laws of the land," Mr. Cheney continued, adding, "They're carried out in a manner that is fully consistent with the constitutional authority of the president of the United States. They are absolutely essential in terms of protecting us against attacks."

Mr. Cheney's sentiments were echoed Friday by two other top administration officials, Treasury Secretary Snow and the White House press secretary, Tony Snow.

The two men, who are not related, defended the program in separate news conferences on Friday. The Treasury secretary called the operation "government at its best," and the press secretary derided criticism of it as "entirely abstract in nature."

The Treasury secretary called the program "an effective weapon, an effective weapon in the larger war on terror."

Administration officials spoke to various reporters about the financial tracking program Thursday night after The New York Times published an article about the program on its Web site. Bill Keller, executive editor of The Times, has said the newspaper decided to publish the story because "we remain convinced that the administration's extraordinary access to this vast repository of international financial data, however carefully targeted use of it may be, is a matter of public interest."

Swift has said that its role in the program was never voluntary, but that it was obligated to comply with a valid subpoena, and had worked to narrow the range of data it provided to American officials.

But the Treasury secretary, Mr. Snow, said Friday that after the Sept. 11 attacks, Treasury Department officials initially presented the cooperative with what he described as "really narrowly crafted subpoenas all tied to terrorism." Officials at Swift responded that that they did not have the ability to "extract the particular information from their broad database."

"So they said, 'We'll give you all the data,' " Secretary Snow said.

Craig S. Smith contributed reporting from Paris for this article, Eric Dash from New York and Laurie J. Flynn from San Francisco.

EXHIBIT E

Privacy International

German Lander Commissioner legal analysis condemns SWIFT transfers to U.S.

25/08/2006

The Data Protection Commission for the German Lander of Schleswig-Holstein released its legal analysis of the SWIFT transfer of transactional data to the US Government. The analysis was released August 23, 2006 and is available for download on the commissioner's website at http://www.datenschutzzentrum.de/wirtschaft/swift/060825_swift.pdf. We have copied the english translation below.

The analysis concludes that the transfers violate German and European data protection law, and calls for the immediate cessation of the mirroring of European data in the U.S. data centre. That is, the analysis sees no reason why intra-EU transactions should be processed at the SWIFT data processing offices in the U.S. and therefore they do not believe that the SWIFT operations in Europe need to be held by the SWIFT offices in the U.S. through any form of mirroring. As such, the data on intra-European transfers should never be within the legal jurisdiction of the U.S. Government.

In this analysis, SWIFT is seen as a data processor for German banks, thus giving the Commission of Schleswig-Holstein jurisdiction over the case.

For intra-European transactions over the SWIFT network (between banks in EU member states), the Commission analysis concludes that the transfer of the data to the U.S. SWIFT data center has no legal basis, and in turn the hand-over of the data to the U.S. authorities is also illegal. The Commission doubts that the use of a contractual clause will assist in clearing up this situation.

From transfers between EU institutions to U.S. institutions (between banks in the EU member states and banks within the U.S.) the Commission's analysis finds that there is no legal basis because of the lack of data protection safeguards in the U.S. The analysis goes on to say that it is the responsibility of German banking institutions to show that the transfer of the data to the U.S. authorities was proportionate, but as no such proof was provided then the transfers are illegal.

Opinion delivered by ICPP on August 23rd, 2006

International wire transfer by Schleswig-Holstein banks using SWIFT

I. Result Summary:

The turn over of European citizens' financial data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) established in Belgium to United

States authorities violates German and European data privacy law.

II. Statement of the Reasons

In international wire transfer the bank receiving an order is responsible for compliance with privacy protection regulations and confidential use of personal data on its way up to the transfer receiving company.

The commissioned banks as far as they have entrusted legally independent companies with data processing especially forwarding of records of wire transfer are responsible to ensure the level of data protection of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) in an unbroken chain all the way up to the data receiving financial institution.

Involving third parties that support the forwarding of client data for the purpose of routing a specific international wire transfer is a case of data processing on a commissioned basis under section 11 BDSG. The bank instructed to transfer money is responsible to provide an unbroken chain of written contracts with all financial institutions involved guarantying a constantly high level of protection as required by the provisions of the Federal Data Protection Act and the data concerned.

SWIFT acts as an agent or subcontractor of the data controller, the members of the SWIFT-group. At present, SWIFT does not give sufficient privacy protection guaranties that would justify handing over personal data to be processed by SWIFT. Particularly missing is a privacy protection measure comparable to the one provided in section 11 BDSG that ensures SWIFT to be bound to instructions and confidential use of entrusted bank customer's data.

SWIFT maintains a database in the United States of America which includes data records of European citizens that do not have contractual relations to U.S. agencies or U.S. banks. The transfer of this data by SWIFT/Europe to SWIFT/U.S.A. still lacks proof of a supporting legal basis. Sole measures to ensure an adequate level of data protection in the U.S. are not sufficient.

The instructing banks also bear a joint responsibility for illegal transfers of personal data by SWIFT to the U.S. and illegal processing of these data in the U.S. because being the responsible mandator, they are obliged to ensure lawful processing in compliance with data protection law.

The turn over of all records or parts of SWIFT customer data by European banks to the U.S. treasury Department or U.S. intelligence services for the purpose to fight terrorism is illegal due to a missing legal basis for respective data transfers.

The protection of the right to individual self determination for international money transfers requires written proof or warranty concerning adherence to adequate data protection standards valid for all companies in the transfer chain.

III. Statement of the Reasons in Detail:

In this case, a distinction is made in respect of data privacy law

1. between data transfer of a company as an instructing institution to the data centres as well as from there
2. to the central giro institutions involved,
3. data transfer between the central giro institutions involved and SWIFT, as well

as

4. data transfer between SWIFT and companies of the respective remittee established in third countries,
5. data transfer between SWIFT/Belgium and SWIFT/U.S.A., and
6. a turn over of entire database records by SWIFT/U.S.A. - according to current knowledge - on the basis of an administrative subpoena by the U.S. Treasury Department to the Central Intelligence Agency (CIA).

Add 1. and 2. Legal basis for data transfer between the financial institution receiving the customer order and the data centres and onwards to the central giro institutions

a. Facts of the case

In order to route international banking transactions on behalf of their clients, Schleswig-Holstein banks have commissioned mostly centralized institutions, the central giro institutions.

IT-wise the majority of Federal German branch banks are connected to and supported by data centres belonging to their own enterprise. Orders to conduct international transfers are usually received by the data centres first and are then forwarded to the respective central giro institution.

b. Valuation

aa. Applicability of Data Protection Law

Addressee of the regulations put down in the Federal Data Protection Act are pursuant to section 2 (4) BDSG private bodies meaning natural or legal persons, companies and other private-law associations. According to section 3 (7) BDSG any person or body collecting, processing or using personal data on his or its own behalf or commissioning others to do the same is to be classified a controller within the meaning of the law. The Federal Data Protection Act does not provide a group privilege. This fundamental decision was reaffirmed by the legislator when passing the amendment of the Federal Data Protection Act in 2001.

Pursuant to section 3 (4) no. 3 BDSG especially the transfer of personal data is defined as the disclosure to a third party by means of data processing either a) through transmission of the data to the third party or b) through the third party inspecting or retrieving data held ready for inspection or retrieval.

The personal data of the individual (the natural person) are exclusively under protection pursuant to section 1 (1) BDSG. Section 3 (1) BDSG defines personal data as any information concerning the personal or material circumstances of an identified or identifiable individual (the data subject).

According to the Central Credit Committee (Zentraler Kreditausschuss, ZKA) most of the international wire transfers are commissioned by companies acting as legal persons yet, out of the up to 12 million SWIFT supported transfers there are millions of daily transactions caused by private individuals (natural persons). Moreover, companies are also protected by the data protection laws as long as identifiable individuals acting on behalf of the companies can be allocated and whose rights to privacy are affected.

Bank clients who order international wire transfers fill in a standardized form. On the basis of this form, the commissioned company prepares a respective international payment transaction notification for the purpose of transmission via the SWIFT

network to the credit institution of the payee. The international payment transaction notifications are set up according to ISO-standards. They comprise among others personal data on the party ordering, the remitee, the amount, and the purpose of use. In a transfer order to a state outside the European Union the address of the person ordering is also included in the data record. The latter are transferred comparable to an email service via a so called Virtual Private Network operated by SWIFT.

bb. Legal Basis

The data transfer at hand needs to be legally justified under section 4 (1) BDSG or has to meet the requirements under section 11 BDSG respectively a cumulative – as far as it is a data transfer to a party not mentioned in section 4b (1) BDSG – justification in pursuance of sections 4b, 4c BDSG.

The collection of data is based on a contract between the financial institute commissioned with international money transfer and the customer as the principle of the order for the purpose of transfer of money to a person in a third country (order to transfer/agency contract). The involvement of data centres or central giro institutions for the performance of the orders is neither covered by the contract nor is the customer usually aware of such involvement. The routing of data takes place between two legally independent parties and requires a separate legal basis pursuant to section 4 (1) BDSG except, a privileged case under section 11 BDSG exists. The commissioned collection, processing or use of personal data in pursuance of section 11 BDSG serves to secure data privacy and data security standards imposed on the controller who chooses to process personal data not on his own premises. The objective is reached by imposing full responsibility of privacy protection on the principle whereas the body commissioned to fulfil the task only serves as an auxiliary body of the principle and is subject to instructions completely. Commissioned data collection, processing, or use is not identical with those business relations between two or more companies referred to as outsourcing. Also, for the classification of data forwarding as commissioned data processing under section 11 BDSG, it is not relevant what kind of civil contract is established between the contractual bodies. The most important criteria for the classification of a commission is the mere auxiliary function of the agent regarding data collection, processing, or use fulfilling the tasks and the business purpose of the controller.

The involvement of the central giro institutions serves - according to current knowledge - the mere function to collect and batch the handling of international payment transactions within the net of branch banks. They do not have the power of decision concerning method and manner of data processing. The baseline method is rather standardized to a large extent. The central giro institutions are used as an extension of the banks focussed solely on the functional execution of the order. Hence, it appears that regarding the relationship between the commissioned citizens' respectively customers' banks and the central giro institution no contrary views are taken. Consequently, they have to be classified as agents under section 11. Clues to detect a transfer of function are not to hand.

The legal basis pursuant to section 28 (1) BDSG, presented by ZKA in its statement from 10.08.2006 that lacks reference in substance concerning the involvement of central giro institutions in lawfully forwarding data up to the remitting financial institute, must fail because the customer cannot see from the underlying transfer order which route and which concrete bodies will get involved performing the international transfer. The underlying relationships between financial institutions for a specific international transaction are not revealed to the customer. Moreover, the underlying chains of transfer involving data centres, central giro institutions, but also occasionally special international payment transactions systems, correspondent credit institutes in third countries as well as on other terms involved financial institutes are unknown to the consumer and are not revealed within the actual

transfer contract with the data subject. Bank clients who engage in international wire transfer are only concluding contractual relations with the specific financial institute they place their order with. Within this framework of valuta ratio it is only transparent to the customer that handling international payment transactions between themselves and the remittee, the remitting financial institute is engaged on the basis of a respective collection relationship between the remittee and the ordered (foreign) financial institution. For these reasons a classification of data forwarding according to sections 4, 28 (1) cl. 1 no. 1 BDSG is not applicable.

The absence of written contracts as required pursuant to section 11 (2) cl. 2. BDSG concerning the necessary privacy protection and data security measures for central giro institutions in their function as commissioners, results in an illegal data transfer to a third party due to the absence of an effective legal basis under section 11 BDSG.

Add. 3 Forwarding of Data between Central Giro Institutions and SWIFT

As has been stated under add. 1 and add. 2, data centres as well as central giro institutions act from the data protection point of view as commissioners of the companies (even though illegal as an effective contractual basis for data transfer under section 11 BDSG is wanting) having initially received orders for international wire transfers from their clients. As commissioners data centres as well as central giro institutions are strictly bound to instructions concerning the use of data entrusted to them for the performance of the order, cf. section 11 (3) cl. 1 BDSG (cf. on this Walz in Simitis, BDSG Commentary, 6th ed., section 11 BDSG, no. 56; Gola/Schomerus, 8th ed., section 11, no. 24).

The central giro institutions involved only perform the commissioned task received from the single banks to forward the incoming international transfer orders as a contractual partner of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to the latter. From the data protection point of view this again constitutes data transfer between legally independent companies that need legal justification. This is to be qualified on the grounds of the underlying sub-commission between banks and central giro institution and their total dependence on instructions as well as the standardization of the mass business processes as commissioned collection, processing, or use of personal data under section 11 BDSG. From this point of view SWIFT can be classified as a subcontractor of the commissioning European banks under Article 17 (2) and (3) of Directive 95/46/EC. Obviously SWIFT does also assume such a classification. Pursuant to item 4.5.3, subsection 4 of the General Terms and Conditions of the company from January 2005, it is pointed out that SWIFT is bound to instructions of their clients especially in forwarding personal data in messages and files and under recognition of the status as data processor according to EC-Directive 95/46. Also, motive 47 of the EC Directive states in cases of messaging a rule imposing privacy protection responsibility on the person from whom the message originates. The data processor is subject to European data protection law and its standards under Article 17 (2) of 95/46/EC.

There are no clues to assume functions to be assigned to SWIFT and therewith of own responsibility as a controller pursuant to BDSG. As stated afore, the commission to receive transfer data in a specific format and to forward them to a third party fulfils subordinate auxiliary functions for the ordering financial institutions' account only. The business terms of the company point out this fact very clearly.

Also, the trans-boarder character within the EU (to Belgium or The Netherlands) constitutes no obstacle to classify the forwarding of data as processing by way of a data processor: this would only be the case if the service provider SWIFT could be classified as a third party in the sense of section 3 (4) no. 3 BDSG. If they were a

third party, it would be classified a data transfer under the BDSG. In this case, the statutory prohibition subject to exceptions by permission pursuant to section 4 (1) BDSG would be applicable. However, according to section 3 (8) cl. 3 this does not include the data subject or persons and bodies commissioned to collect, process or use personal data in Germany, in another member state of the European Union or in another state party to the Agreement on the European Economic Area. This privilege is restricted to recipients of personal data within the territory of the European Union or European Economic Area (EWR).

The written contract to be presented by the commissioning bank (see on this item 1 and 2) has to include specific stipulations concerning the admissibility of subcontracting – in this case SWIFT – so that data centres and central giro institutions are enabled to conclude a respective sub-commission concerning the further processing of the data entrusted upon them. Otherwise they would lack power to engage further bodies with data processing without the permission of the principle. There would be a risk that responsibility for legality of data processing "vanishes" respectively that the standard of data security verified by the principle and given in writing are undermined (cf. Simits-Walz, ibid. no. 52).

Subcontracting can only be allowed by the commissioning banks if the agent – in this case data centres and central giro institutions – ensure and if necessary also prove that they comply with their obligations and that the subcontractor observes privacy and data protection standards as stipulated (cf. Simitis, ibid. no 52). The principle stays responsible as a controller of data processing even in relation to the subcontractor. The agent placing the order with the subcontractor has to stipulate this by contract and has to ensure that the principle can actually execute the obligation to check on the subcontractor (cf. Gola/Schomerus, ibid, no 27).

The fact that SWIFT seems to be the only service provider supporting specific methods to move money abroad has no relevance concerning its legal classification as data processor. Otherwise the level of privacy protection using third party services to be provided by financial institutions would be subject to market conditions. As far as the objection raises the impression a sufficient influence on the business terms of SWIFT is missing, this is clearly contradicting the legal construction of SWIFT that is operated according to its structure by the cooperative financial institutions themselves. Therefore, proof of unsuccessful attempts of German financial institutions in the coordinating committee of SWIFT expressing a demand of improvements according to the privacy protection law in force in SWIFT is missing.

Furthermore, it is necessary to contractually stipulate an obligation of the agent as well as of the subcontractor to notify the principle in cases of privacy and data security relevant obstructions of processing respectively contractually relevant incidents.

At present there are no agreements such as required under section 11 BDSG between the central giro institutions commissioned by single banks and their business partner Society for Worldwide Interbank Financial Telecommunication (SWIFT), classified a legal subcontractor from the point of data privacy law. Especially SWIFT General Terms and Conditions of January 2005 as well as their Data Retrieval Policy of May 26, 2006 do not include any terms that would implement the requirements concerning privacy and data security under section 11 BDSG. Explicit written stipulations are missing concerning a strict obligation to act only on instructions from the principle. On the contrary, the terms and conditions as well as the Retrieval Policy provide a contractual framework that raise reasonable doubts concerning the legal validity of the commission from the privacy point of view because of two reasons:

1. The General Terms and Conditions refer to further product related information and general terms that are not available. Especially sufficient information is missing stipulating the requirements under section 9 BDSG and under the Annex to section 9 BDSG. Without any further information it cannot be

assumed that SWIFT/Europe transfers personal data in compliance with the law in force.

2. Having in view the international activities and presence of SWIFT and the connection between SWIFT/Europe and the Operating Centres of SWIFT/U.S.A. sufficient transparency concerning if and to what extend at which locations personal data of European respectively German citizens respectively bank clients are stored and processed is necessary. This is especially true for any legally independent service provider engaged by SWIFT who gains access to personal data from SWIFT's databases. Only on this basis, the principles of the orders can decide whether and to what extent sufficient measures are taken by SWIFT concerning third country transfers under Article 25 and 26 of Directive 95/46 respectively sections 4b, 4c BDSG to ensure the legality of data processing. These safeguards affect the legality of data transfer concerning the adequate level of protection in third countries only.
3. Missing is the principles right to check on the technical and organisational measures taken at the locations in compliance with section 11 (2) cl. 3. BDSG. At present, such a right is obviously only granted to SWIFT in relation to its own clients, in this case the central giro institutions, according to item 4.5.5. subsection 2 of the Terms and Conditions.
4. Item 3.5.3 of the Terms and Conditions grants SWIFT the right to change services and products at any time if respective changes are required by any regulatory authority. This clause is not sufficiently specified. It is not clear whether the designated authorities are only to be national (Belgium) authorities or whether authorities from third countries are granted a similar status. Since respective orders from authorities can affect the technical and organisational protective measure concerning personal data processing, an explicit proviso of legality in compliance with the basic rights of EU-citizens is necessary.
5. Item 3.2 of the Data Retrieval Policy (Mandatory Requests) is not sufficiently determined. It also raises the question under item 4. concerning the specific authority nominated. On the other hand and having in mind any claims for turn over of personal data from insecure third countries, a contractual obligation to notify the directly affected clients/principles preliminary and without delay in order to perform and coordinate the turn over to the extend necessary. Having in mind illegal claims, an obligation to check the substantive law concerning claims for turn over of personal data should always be stipulated with the subcontractor including his right to reject such a claim until a legal investigation of the matter has taken place. In any case, the agent is obliged to resist obviously illegal claims and to agree with the principle upon a legal solution if necessary.

   This standard is necessary because for EU-citizens can rely on data transfers of customer data only taking place between companies established within the country (respectively within the EU) and foreign authorities on the basis of bilateral (e.g. treaties providing for mutual judicial assistance) or international treaties *in individual cases*.
6. The Data Retrieval Policy of May 26, 2006 explicitly referring to the legality to turn over data on the ground of a so called "bona fide subpoena or other lawful process by court or other competent authority" states that there are no preceding versions so far making a review of the lawfulness of the preceding period since 2001 impossible. As far as the term bona fide subpoena should include an administrative subpoena by the United States Treasury Department such as issued in the present case, objections also exist concerning due process as regards similar claims to turn over data in Germany. The latter can only be issued on the grounds of a valid individual court-approved warrant or subpoena (cf. hereinafter add. 6).

Add. 4. and 6. Data transfer between SWIFT and Remittees

established in the United States (U.S. related transfer orders) respectively Operating Centres in the U.S.

The bank statements distinguish between data transfer into the U.S. on the grounds of U.S. related payment orders and data transfer without U.S. reference that only occur as complete data records are mirrored to the U.S. Operation Centre.

1. **Forwarding of Data on occasion of U.S. related payment orders**

Forwarding of data on occasion of a money transfer by SWIFT to a remittee established in the U.S. is always a data transfer from the point of privacy law irrespective of privileged data processing by way of a processor within the EU. This classification is according to the prevailing opinion, drawn from a reversed conclusion from section 3 (8) cl. 3 BDSG (likewise ZKA, Statement, p. 5, section 4).

According to the facts of the case, it is not sufficiently substantiated whether the performance of a U.S. related transaction always leads to a turn over of data to SWIFT/U.S.A. This forwarding of data would also be qualified as data transfer respectively disclosure to third parties under section 3 (8) cl. 3 BDSG. Yet, the foreign branch of the controller is not mentioned explicitly as a third party. Foreign branches in third countries are pursuant to the prevailing opinion qualified as third parties as well because the legislator did not want personal data of data subjects to be dismissed from the harmonized protection of Directive 95/46/EC without compliance to the legal requirements of data transfer (cf. Simitis-Dammann, ibid, section 3 no 247 and Simitis-Simitis, ibid, section 4b, no. 17 with further references).

Data transfer into the U.S. needs to be based on a sufficient BDSG legal basis pursuant to section 4 (1), 4b (2), cl. 1 which can be derived from the initial bank clients transfer order pursuant to section 28 (1) cl. 1, no. 1 BDSG. This is undoubtedly a valid legal basis in cases of direct data transfer between the customer bank and the U.S. bank of the remittee without any further transfers to SWIFT/U.S.A. in between. Insofar, only the initial payment order between the German-based principal and the remittee established in the U.S is performed. The German-based bank receiving the customer order initially remains data controller of the data transfer in the sense of section 3 (7) BDSG. With regard to this relationship the customer is aware of his order relevant data being transferred to the United States.

The requirements numerated in sections 4b, 4c BDSG as of the afforded level of protection in the recipient country must be stated. Forwarding personal data into the U.S. is, in pursuance with section 4b (2) cl. 1 BDSG, a transfer of personal data to other bodies abroad (third countries) for which an adequate level of data protection must generally exist in recipient country. The adequacy of the afforded level of protection is generally assessed under consideration of the circumstances enumerated in section 4b (3) BDSG. In the present case, this consideration may be left open because the exemption named in section 4c (1) no. 2 BDSG being subject to strict interpretation concerning transfer necessary for the performance of a contract between the data subject and the controller is applicable (cf. on transfer abroad as a typical example Simitis-Simitis, ibid, section 4c no. 13).

As far as the realisation of data transfer is necessarily relying on the services of service providers or branches within the U.S. proof of an adequate level of privacy and data protection performed by these enterprises is still missing (cf. on this hereinafter).

1. **Forwarding of Data without U.S. Relation/Mirroring data records into the U.S.**

The forwarding of German customer data by SWIFT/Europe to SWIFT/U.S.A. without

a U.S. relation – e.g., transactions within Europe that are only transferred for security reasons to the Operation Centre U.S.A. – is subject of a two level admissibility check. This can be, as already stated above, a data transfer from the initially responsible and commissioned bank that only uses the SWIFT infrastructure as a tool.

In this case scenario, doubts already arise from the point of admissibility with regard to the legal basis from section 4, 28 BDSG. A legal justification in pursuance of section 28 (1) cl. 1, no. 1 BDSG fails due to the lack of specific and objective necessity of data transfer into the U.S. for the winding up of the contract (cf. the criteria Simitis-Simitis, section 28, ibid, no. 91, 92). The only purpose for the data transfer into the U.S. is as stated so far to serve the structure of data security as developed in SWIFT. This purpose does not serve the routing of a transfer order because the respective transfer goal can be achieved without it being forwarded to the U.S.. The mere fact of this security infrastructure opposed to legislative ratio does not justify another evaluation result. If and as far as concerning the necessity of data transfer respective related protective measures for the compliance with German protective standards would be implemented, data transfer even to SWIFT/U.S.A. could be admissible. For SWIFT/U.S.A. this would require protective measures similar to those in section 11 BDSG. Further, an adequate level of protection for SWIFT/U.S.A. according to the measures provided by European data protection law has to be created. Additionally, it seems possible that data transfer into the U.S. can be developed as a black-box procedure using encrypted data that can not be accessed by SWIFT/Europe without a respective binding instruction from the relevant cooperative head office respectively which cannot be turned over offhand.

At present, the data transfer concerning the requirement to provide an adequate level of protection in the recipient country is illegal: insofar, an adequate level of protection should at least be ensured in respect of the data processing taking place at the Operating Centre of SWIFT/U.S.A.. Since for the U.S. no binding statement with regards to the adequate level of protection pursuant to Article 31 (2) of the EU Data Protection Directive 95/46 exists and according to the current state of information, SWIFT did not accede to the Safe Harbour Principles (cf. on this Simitis-Simitis, ibid, section 4b, no. 70 ff.) and as to current knowledge an exceptional permission has not been issued by an authority under section 4c (2) BDSG, data protection guaranties as granted to EU citizens are missing regarding data transfers to SWIFT/U.S.A..

The standard contractual clauses of September 16, 2005 between SWIFT/Europe and SWIFT/U.S.A. as known to ICPP do not provide an adequate level of data protection in the recipient country. For according to Annex B of the contract, it involves a legitimization of data processing especially relation to SWIFT employees. This also follows from the chosen contractual master "controller to controller" based on the decision 2001/497/EC. Obviously, own standard contractual clauses legitimating the transfer of data from the European principle into the U.S. do not exist.

Any data transfers for data security purposes from SWIFT/Europe to SWIFT/U.S.A. on the grounds of the material and information at hand are to be assessed as illegal.

The explanations concerning the necessity to upkeep an active fall-back-system within the frame of a security concept of the company do not lead to a different judgement. On the one hand the explanations do not concern the so called first level check according to BDSG that is admissibility of data transfer. Insofar, a sound explanation referring to a sufficient legal basis is missing.

On the other hand the data security infrastructure does not *directly* belong to the transactions that are necessary regarding the execution of a transfer order within Europe for a data transfer under section 4c (1) no. 2 BDSG.

Over and above this, a statement explaining why and for which explicit purposes a)

databases are necessary for the network infrastructure of SWIFT respectively what kind of indispensable tasks they perform and b) why it is essential to establish them in the U.S.. ICPP is not aware of any other comparable cases of fall-back-facilities that of all vitally need intercontinental data mirroring of the total data pool.

The contractual agreement between the German financial institutions and SWIFT, as referred to in the ZKA letter of August 10, 2006, does on no account singularly provide an adequate level of protection that would legalize the data transfers into the U.S. for the purpose of mirroring. Especially wanting on the first check level is a comparable level of protection in compliance with the requirements of section 11 BDSG. Moreover, in order to ascertain the adequateness of the level of protection it is necessary for instance to use the instruments provided by the EU-commission or to ask the respective competent authority for an exceptional permission.

Basic concerns incidentally exist against contractual solutions also supported by standard contractual clauses if and to the extent to which the third country does not provide protection against governmental access to personal data in a way corresponding to the level of protection within the EU. Insofar the use of standard contractual clauses as a guaranty under section 4c (2) cl. 1 BDSG and Article 26 (2) Personal Data Protection Directive 95/46/EC and data transfer to third countries is disqualified (cf. Dammann-Simitis, Commentary EU Data Protection Directive, Art. 26, no. 16). At this point major concerns currently even exist in the U.S. regarding the regulations developed by the U.S. Treasury Department to turn over records of international wire transfers.

Turn over of data records by SWIFT to U.S. Authorities or the CIA

1. **Facts of the Case**

According to the statement of ZKA of August 10, 2006 which is based on the statement of a spokesperson from the U.S. Treasury Department, only "a subset of its records" has been turned over on the basis of a so called administrative subpoena issued by the U.S. Treasury Department. It was alleged that the records were drawn entirely from a SWIFT/U.S.A. database on U.S. territory. In the ZKA statement it is emphasized under item I.5 that according to statements of the U.S. Treasury Department no data records from the server of the European Operating Centre have been turned over. Moreover, the ZKS statement refers to a framework agreement between SWIFT and the U.S. Treasury Department which is obviously available to SWIFT and its affected members and which from an unspecified date onwards – according to press records probably since 2003 – includes terms for data transfer to U.S. authorities.

The facts of the case raise a number of further issues. As far as the ZKA refers to an unavailable framework agreement between SWIFT and the U.S. Treasury Department, it causes amazement. At least one of the affected members being a legally responsible contractor and responsible member of SWIFT should be allowed to receive or produce a copy of the said framework agreement. As long as this agreement is not presented and reliable facts concerning the date on which the agreement was concluded are not available, it cannot be taken into account for the further legal assessment. It is not understandable why an agent who enters into a secret agreement negotiates the conditions of turn over of sensible financial data entrusted to him by numerous clients and who is organised and lead as a cooperative, is not able to clarify the current and historical facts of the case and to produce the relevant documents.

According to media records relating to the issue, especially an article published in the New York Times on June 23, 2006, the said agreement between SWIFT and the U.S. Treasury Department is only in effect since 2003. Before this date the U.S. Treasury Department is

said to have had full access to the complete records of SWIFT. The so called administrative subpoenas have only been issued to give SWIFT a minimum of legal certainty for the turn over of records. Only in 2003, executives at SWIFT had legal concerns grown to an extend that made them ask for a further reduction concerning the transfer of data. The so called administrative subpoenas as a legal basis for the turn over of records are still highly disputed as reported in the N.Y.T. on June 23, 2006 as well as in the Los Angeles Times on June 24, 2006. According to these reports, law enforcement officials have relied on grand-jury subpoenas or court-approved warrants until 9/11. Ever since this incident administrative subpoenas became frequent. This account of the facts is still not refuted.

Concerning the press reports on SWIFT, a secret Bush administration eavesdropping program also relying on broad administrative subpoenas of the U.S. President with reference to his war against terror is often mentioned. In this respect, it is to note that in the meantime and according to a press report on August 17 (Spiegel-Online, August 17, 2006) a circuit court in Detroit/Michigan/U.S.A. has revoked the actions of U.S. authorities because they did not seek court-approved warrants.

The statement of ZKA in reference to a statement of a U.S. Treasury Department employee, according to whom data from the server of the European Operating Centre has not been turned over, is not understandable. His statement can neither be found in the cited statement of Mr. Levy, Under Secretary Terrorism and Financial Intelligence U.S. Department of the Treasury, before the House Financial Services Subcommittee on Oversight and Investigations nor can it be detected in other press reports. On the contrary, this assumption is contradictory to the ZKA statements (bottom of page 5) according to which payment orders of European citizens not related to the U.S. could be found in the U.S. Operating Centre due to the procedures of the SWIFT data security concept including full data mirroring. It has to be assumed that these data records on solely European transactions were subject to the examinations by U.S. authorities.

The ZKA statement does not mention the fact that the data turned over by SWIFT did not concern transfer data about specific individually accused suspects but about a complete or partial turnover – eventually since 2003 – of all information available to SWIFT on transfer orders of their clients lasting for at least five years and has not been stopped ever since.

2. Valuation

It has already been stated above that SWIFT is acting as an agent on behalf of the financial institutions (principal-agent relationship). As an agent SWIFT is strictly bound to instructions concerning personal data entrusted to her. The financial institution always stays responsible as a controller when forwarding or transferring such data to third parties. Insofar, the financial institutions established in Germany using the SWIFT network are responsible to check the general terms and conditions and data retrieval policy as regards contradictions and infringements of guarantied protective standards and to bring on the necessary adaptations.

The turn over of inner European transfer orders, unnecessarily transferred to the U.S., to U.S authorities, lack a legal basis because the transfer of these data to SWIFT/U.S.A. without a sufficient legal basis constitutes an unlawful act. These data should not have been accessible to U.S. authorities on U.S. territory in the first place.

There are also no sufficient measures taken, especially from the measures provided by the EU, to establish an adequate level of protection by SWIFT/U.S.A. Even if EU standard contract clauses would have been chosen basic concerns about the adequate level of protection would still prevail. As long as there is no protection against state access to personal data guaranteed that corresponds to the European level of protection, contractual clauses on the transfer of personal data to third countries are not sufficient as a guarantee pursuant to § 4c (2) cl. 1 BDSG and Art. 26 (2) of Directive 95/46/EC (cf. Dammann-Simitis, Commentary on the EU-Directive, Art. 26, no. 16). Insofar, significant concerns exist as regards the administrative subpoenas issued by the U.S. Treasury Department. The issue is also subject to disputes in the U.S.

Even in case information on transfer orders with regard to the U.S. are claimed by U.S.

authorities from SWIFT/Europe, the principle in Germany stays responsible to check the claim as long as the disposal of data is still under the authority of the agent. Because the agent SWIFT is acting across boarders and in an – from the data protection point of view – insecure third country, the agent has to prove that the data centres involved provide sufficient data protection measures. This could be achieved with regards to compliance with BDSG protection standards by changes in the Data Retrieval Policy of SWIFT as outlined in item 3. and 4.

Pursuant to section 28 (3) no. 2, 28 (6) no. 3 BDSG such data transfer to public bodies is legitimate if no reason exists that outweighs the data subject's interest in excluding turn over. The BDSG requires a decision that is subject to a weighing of reasons by the controller who has to make use of all available information to ensure that the requirements for the claim are met. The commissioned collection, processing or use of personal data requires that the principle ensures a respective obligation of the agent in writing (cf. on this proviso 5d on standard contractual clauses for commissioned data processing, Decision by the Commission 2002/16/EC).

Single data records should have only been turned over after consulting the affected financial institutions. The – substantive - obligation to check the claim of the U.S. Treasury Department should have resulted in a rejection to comply with the claim concerning the scope of data and the duration of the measure being obviously unlawful.

The violation of data protection law and the responsibility for the unlawful turn over of data by SWIFT also rests with the financial institutions in Schleswig-Holstein having accepted transfer orders from Schleswig-Holstein citizens. In terms of data privacy law they are responsible for the chain of companies involved to guarantee confidentiality of the data entrusted to them by their clients for a specific purpose.

Related:
Anti-Terrorism Policy Home Page
Policy Laundering Home Page
Europe's Privacy Commissioners rule against SWIFT
Swiss Privacy Commissioner claims SWIFT and Swiss banks infringed privacy law
Belgian Prime Minister condemns SWIFT data transfers to U.S. as 'illegal'
An Open Letter to the CEO of SWIFT on other covert programmes for access to financial data
European Parliament resolution on SWIFT builds on PI work
PI and ACLU show that SWIFT auditor has extensive ties to US Government
Pulling a Swift one? Bank transfer information sent to U.S. authorities
Briefing on FATF and Financial Surveillance
PI commences legal action to suspend unlawful activities of finance giant

<< Back

Privacy International, 6-8 Amwell Street, Clerkenwell, London EC1R 1UQ UK. Email us at privacyint@privacy.org.
Call on +44 (0)208.123.7933 or +1.202.470.0099.
Privacy Policy - About PI - Support PI

EXHIBIT F

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

The Federal Data Protection and Information Commissioner
FDPIC

Access to SWIFT Transaction Data –
Opinion of the Federal Data Protection and Information Commissioner

I. Introduction

Most international payment transactions are processed by the Belgian-based *Society for Worldwide Interbank Telecommunication* (SWIFT). In June of this year the media revealed startling information according to which the US administration had obtained access to SWIFT transaction data within the context of its efforts to combat terrorism.

From a legal perspective, data protection is quite clearly one of the central issues. This explains why the data protection authorities of numerous countries have sought clarification. As SWIFT is headquartered in Belgium, the investigation by the country's *Commission de la protection de la vie privée* is of particular importance. The Privacy Commission published the result of its work on 27 September 2006.

After receiving information about these developments from the press, the Federal Data Protection and Information Commissioner (FDPIC) contacted the most important players in the Swiss banking sector to obtain more details. The present opinion is based on the knowledge thus gained, on the Belgian report[1], as well as on the position of the Swiss Federal Council for the attention of the Control Committee of the lower house of the Swiss parliament of 4 July 2006.

The Federal Council's position paper not only sets out the salient facts, but also allocates responsibility to different bodies to determine the lawfulness of the transactions. Thus it is up to the FDPIC to determine whether the provisions of the Data Protection Act have been respected, whereas the courts have jurisdiction over matters involving an infringement of Swiss bank secrecy laws[2].

From a strictly legal perspective, the principle of territoriality adds a further restriction to the scope of the opinion. According to our sources, SWIFT does not process any *personal data* in Switzerland[3]. Therefore SWIFT falls under Belgian and not Swiss data protection legislation. The Belgian Privacy Commission did, however, rightly remark that because of the interaction between SWIFT and the financial service providers, there is a shared responsibility for the data processing[4].

---

[1] *Opinion no. 37 / 2006 of 27 September 2006 relating to the transfer of personal data by the SCRL SWIFT following the UST (US Department of the Treasury) subpoenas.* Referred to hereinafter as the "Belgian report". The full text may be found under www.privacycommission.be.

[2] In this context, the Federal Council considered that the Swiss National Bank (SNB) and the Swiss Federal Banking Commission (SFBC) were not competent to determine conformity with the law.

[3] Neither *SWIFT Switzerland GmbH* nor the *SWIFT Switzerland National Member and User Group* are involved in any activities relating to the processing of transaction data on behalf of the Belgian SWIFT.

[4] cf. Belgian report, page 14 f.

Feldeggweg 1, 3003 Bern
Tel. 031 322 43 95, Fax 031 325 99 96
www.edoeb.admin.ch

As the national authority, our primary task is to determine the data protection responsibility of the financial service providers in Switzerland without losing sight of the bigger picture. Thus, although our primary task is to consider the behaviour of SWIFT, our conclusions should not be limited to the situation in Switzerland. The issue has acquired an international dimension, and simply considering the problem from a national data protection perspective does not go far enough.

II. SWIFT's responsibility

After 9/11 and the attacks on New York, SWIFT found itself confronted with different (and often irreconcilable) legal systems (Belgian, EU, US). As the Belgian report shows, SWIFT decided that it would essentially comply with US law. Although in its negotiations with the US administration, and more specifically with the *US Department of the Treasury*, SWIFT did seek to secure greater control and influence[5], in the final analysis it nevertheless violated Belgian and European data protection law in a number of areas[6].

As SWIFT and the financial service providers have a shared responsibility for ensuring that the payment system complies with data protection laws, the extent of SWIFT's dereliction of duties is highly relevant when it comes to analysing the situation in Switzerland.

Insofar as the duty to inform is concerned, the fact that several players are involved is of particular relevance. Even if we leave aside the argument as to the legality of the US administration gaining access to the data, there is a serious data protection issue due to the lack of transparency of the process for the data subject. On this particular point the joint responsibility for data processing must be considered separately for SWIFT and the financial service provider.

On the subject of the obligation to adhere to the principle of transparency when processing data, the Belgian authorities came to the conclusion that SWIFT should have informed the financial service provider and the data protection authorities about the application of US subpoenas on SWIFT and the possibility of access to data by the US authorities[7].

Within this context, we also need to ask whether the financial service providers failed in their duty to inform as well. It should not be forgotten here that within the SWIFT payment system it is the financial service providers, and they alone, who actually have contact with the individuals concerned. If transparency is to be guaranteed in individual cases, it stands to reason that the financial service providers need to be reminded that they are bound by certain duties.

[5] cf. *Belgian report*, p. 6 f.
[6] cf. *Belgian report*, p. 16 ff.
[7] cf. *Belgian report*, p. 23 f.

III. The responsibility of financial service providers in Switzerland

When a payment transaction is effected via a financial institution, the payor and the payee must be known. If a financial service provider in Switzerland participates in a payment transaction, it may be assumed that this will involve the processing of personal data within the meaning of the Swiss Data Protection Act (Article 3, letters a and e of the DPA). Thus, the financial service provider is subject to all the duties which the Data Protection Act applies to private individuals (DPA and the Ordinance relating to the Data Protection Act – VDSG).

As indicated earlier, the issue of a potential breach of duty also raises another important question regarding the failure to provide appropriate information. More specifically, we need to ask whether the financial service provider has respected the principle of good faith with regard to the processing of the data (Article 4, paragraph 2 DPA).

We have already stated that the degree of knowledge of the financial institute is of decisive importance in this respect. If the financial service provider was aware that SWIFT had transferred data to a third party, then it was bound by the Data Protection Act to inform the person concerned. The statutory requirement that data processing be made transparent is respected only if the data subject is informed about subsequent data processing steps[8]. Given the chronology of a payment transaction, the duty to inform can only apply to the financial service provider who acts on behalf of the payor.

It should be noted that the duty to inform applies even if there *merely a possibility* that a third party may gain access to SWIFT data. It is not necessary, or perhaps even possible, to acquire more detailed knowledge. Even the Belgian Privacy Commission was not able to determine the extent to which the US administration had gained access to the transaction data[9].

The obligation to ensure transparency in data processing continues to apply. The fact that the public has been informed that SWIFT data has been transferred to the US authorities is of no consequence in this regard. Even after the media revealed the story, it cannot be assumed that the general public knows that SWIFT continues to transfer data.

On the other hand, since the publication of the Belgian Commission's report, we now know for certain[10] that SWIFT also processes its data in the USA. This means that data are being transferred to a country in which the level of data protection is not equivalent to that provided in Switzerland (Article 6 paragraph 1 of the DPA). Financial service providers can no longer claim that they are not aware of this situation.

---

[8] The duty to create transparency must be considered within the context of alternative international payments systems that are not channelled through SWIFT. cf. *Belgium report*, p.3

[9] cf. in particular *Belgium report*, p. 6

[10] This was in fact disclosed on various occasions in the past by the media.

IV. Conclusions

- The Belgian Commission's investigations revealed several infringements of Belgian and European data protection laws. On the strength of these disclosures, Swiss data protection laws must also have been infringed. The duty to ensure transparency in data processing has not been respected, nor have the requirements set out in Article 6 of the DPA been fulfilled.
- We concur with the conclusions reached by the Privacy Commission in its report. Any solution which contributes to the battle against terrorism, but which at the same time respects the national data protection legislation of countries which use the SWIFT system, should have been the subject of political negotiations. From a Swiss data protection perspective this is a matter which still calls for action.
- In view of the overall situation, financial service providers in Switzerland clearly are not doing enough to comply with the requirement that they contribute to greater transparency. As was the case with airline passenger data, negotiations are needed in order to improve the situation. What we should be seeking is a solution which not only takes into account US law, but also respects European data protection standards.
- We would appreciate it if the Swiss banks, through their representatives in the SWIFT Switzerland and Liechtenstein national member group, could help bring us closer to this goal if they gave their full support to such efforts.
- Within the context of our co-operation with European data protection authorities, and in particular with the Article 29 Data Protection Working Party, we shall also endeavour to work for a solution that is in conformity with our data protection legislation, and more specifically with the requirements of Article 6 of the DPA.

EXHIBIT G

ARTICLE 29 Data Protection Working Party

01935/06/EN
WP128

Opinion 10/2006
on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Adopted on 22 November 2006

Executive Summary

This opinion of the Article 29 Working Party contains the findings on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

In this context, the Article 29 Working Party emphasizes that even in the fight against terrorism and crime fundamental rights must remain guaranteed. It insists therefore on the respect of global data protection principles.

SWIFT is a worldwide financial messaging service which facilitates international money transfers. SWIFT stores all messages for a period of 124 days at two operation centres, one within the EU and one in the USA – a form of data processing referred to in this document as "mirroring". The messages contain personal data such as the names of the payer and payee. After the terrorist attacks of September 2001, the United States Department of the Treasury ("UST") issued subpoenas requiring SWIFT to provide access to message information held in the USA. SWIFT complied with the subpoenas, although certain limitations to UST access were negotiated. The matter became public as a result of press coverage in late June and early July 2006.

As a Belgian based cooperative, SWIFT is **subject to Belgian data protection law implementing the EU Data Protection Directive 95/46/EC ("the Directive"). Financial institutions in the EU using SWIFT's service are subject to national data protection laws** implementing the Directive in the Member State in which they are established.

The Working Party concludes that:

- **Both SWIFT and instructing financial institutions share joint responsibility, although in different degrees, for the processing of personal data as "data controllers" within the** meaning of Article 2(d) of the Directive.
- **Continued processing of personal data, knowing the large scale of the UST subpoenas, is a further purpose which is not compatible with the original commercial purpose for which the personal data have been collected, within the meaning of Article 6(1)(b) of** the Directive.
- **Neither SWIFT nor the financial institutions in the EU have provided information to data subjects about processing of their personal data, in particular as to the transfer to** the USA, as required under Articles 10 and 11 of the Directive.
- **The control measures put in place by SWIFT, in particular regarding UST access to the data, in no way replace the independent scrutiny that could have been provided by** supervisory authorities established under Article 28 of the Directive.
- **As far as the transfer to the US operating centre is concerned, SWIFT cannot rely on Article 25 of the Directive to legitimate the processing.**
- **None of the derogations in Article 26 (1) of the Directive apply to the processing of data** in the USA.
- **SWIFT did not make use of the mechanisms under Article 26(2) of the Directive to obtain authorisation from the Belgian data protection supervisory authority for the processing operations.**
- **The Article 29 Working Party calls upon SWIFT and the financial institutions to take** measures in order to remedy the currently illegal state of affairs without delay.
- **Furthermore the Article 29 Working Party calls for clarification of the oversight on SWIFT.**

The Article 29 Working Party will follow-up and monitor all of the above.

TABLE OF CONTENTS

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Articles 29 and 30 paragraphs 1 (a) and 3 of that Directive,

having regard to its Rules of Procedure and in particular to Articles 12 and 14 thereof,

has adopted the present Opinion:

1. BACKGROUND

The independent data protection supervisory authorities within the European Union[2] are assessing a major question relating to the transfer of financial data on a large scale from a company based in the European Union (SWIFT) to the US authorities. The details and conditions of such transfers, in particular the processing of personal data relating to individuals in Europe, have raised the concerns of DPAs who have joined forces in the investigation of the data flow and the analysis of its compliance with European privacy principles, in particular with the Data Protection Directive ("the Directive").

1.1. Sequence of events

At the end of June and beginning of July 2006, press coverage in the European and US media questioned the role and responsibilities of the Society for Worldwide Interbank Financial Telecommunication (SWIFT) in relation to the transfer of personal data to the Office of Foreign Assets Control (OFAC) of the United States Department of the Treasury ("UST"). SWIFT is a Belgian based cooperative active in the processing of financial messages. It was revealed that personal data, collected and processed via the SWIFT network for international money transfers using the bank identification code ("BIC") or "SWIFT" code, had been provided to the UST since the end of 2001 on the basis of subpoenas under American law for terrorism investigation purposes.

---

1 Official Journal no. L 281 of 23/11/1995, p. 31, available at http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm

2 In addition to the EU authorities, other data protection supervisory authorities have started investigations on this issue: Australia, Canada, New Zealand, Switzerland, Iceland.

SWIFT released a first statement[3] on 23 June 2006 pursuant to this press coverage. According to its press statement, SWIFT is "the industry-owned cooperative supplying secure, standardized messaging services and interface software to over 7,800 financial institutions worldwide."

The European Commission decided to follow this case closely and asked the Belgian authorities in July 2006 for information about the conditions under which SWIFT processes personal data and whether it complies with Belgian data protection legislation implementing Directive. The Commission is also verifying with Member States whether banks making use of SWIFT for execution of payments orders comply with their national laws on data protection with respect to their processing of personal data relating to such payments.

By resolution of 6 July 2006[4], the European Parliament asked the Member States to ensure and verify that there is no legal lacuna at national level and that Community data protection legislation also covers central banks. In this resolution, the European Parliament also expressed serious concerns as to the purposes of the transfer of data to the UST. It also strongly disapproved of "any secret operations on EU territory" that affects the privacy of EU citizens. It furthermore declared that it is deeply concerned that such operations should be taking place without the citizens of Europe and their parliamentary representation having been informed. It finally urged the USA and its intelligence and security services to act in a spirit of good cooperation and notify their allies of any security operations they intend to carry out on EU territory. The possibility of transfers linked to "illegal activities" was raised but also of transfers of "information on the economic activities of the individuals and countries concerned", which "could give rise to large-scale forms of economic and industrial espionage". The resolution requested the Member States to transmit the results of their verification to the European Commission, the Council and the European Parliament.

On 27 July 2006, the Chairman of the Article 29 Working Party announced that the European data protection authorities had decided to coordinate their activities. In a subsequent meeting on 26 and 27 September 2006, the Article 29 Working Party held a first plenary discussion.[5]

On 4 October 2006, at a public hearing held by the European Parliament's Civil Liberties and Economic and Monetary Affairs committees, the issue was discussed with, amongst other participants, the Chief Financial Officer of SWIFT and the European Central Bank[6].

---

[3] "SWIFT statement on compliance policy", published on http://www.swift.com/index.cfm?item_id=59897

[4] European Parliament resolution on the interception of bank transfer data from the SWIFT system by the US secret services (P6_TA-PROV(2006)0317)

[5] Article 29 Working Party press releases: Press Release of the Article 29 Working Party on Swift Case of 28/7/2006: http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_28_07_06_en.pdf; Press Release on the SWIFT Case of 27/9/2006; http://ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_Swift_Affair_26_09_06_en.pdf .

[6] The full public hearing exchanges can be found at http://www.europarl.europa.eu/news/expert/infopress_page/017-11292-275-10-40-902-20061002IPR11291-02-10-2006-2006-false/default_en.htm

The European Data Protection Supervisor issued some preliminary comments on his investigation into the role of the European Central Bank (ECB) pursuant to Regulation (EC) 45/2001.[7]

At national level, data protection supervisory authorities contacted their relevant banking organizations.

The Data Protection Authority (DPA) of Belgium carried out an inquiry into the legality of the data processing by SWIFT. In the course of this inquiry, the Belgian DPA made direct contact with SWIFT to determine both the scope and scale of the monitoring and the data transfers. The Belgian DPA established in its decision of 27 September 2006 that the transfer by SWIFT of personal data to SWIFT's US branch is in breach of the Belgian law of 8 December 1992 concerning the protection of privacy with regard to data processing of a personal nature[8]. In particular the Belgian DPA found that SWIFT infringed essential provisions relating to the obligations of information, limitation of the purpose of the data processing activities and transfer of the personal data to third countries. The Belgian DPA established that SWIFT made a *"hidden, systematic, massive and long-term violation of the fundamental European principles as regards data protection"*.

On the basis of the information gathered during these investigations the Working Party wishes to analyze the compliance by SWIFT with the data protection principles that are contained in the Directive and implemented in all Member States by national data protection laws with a broad scope of application.

SWIFT sent a copy of its replies to the Belgian, Spanish and French DPA to the Chairman of the Article 29 Working Party[9].

1.2. Facts

1.2.1. SWIFT data processing activities in figures

SWIFT processes an average of 12 million messages on a daily basis[10]. The total volume of messages processed amounted, e.g. in the year 2005, to 2.5 billion messages, of which 1.6 billion were for Europe and 467 million were for the Americas. The information processed by SWIFT concerns messages on the financial transactions of hundreds of thousands of EU citizens. European financial institutions (not limited to banks) use the SWIFTNet FIN Service for the worldwide transfer of messages in relation to financial transfers between financial institutions. This transfer occurs regardless of whether the messages are processed within the European Union (EU) and the European Economic Area (EEA) or in a third country.

---

7 http://www.edps.europa.eu/Press/EDPS-2006-10-EN%20swift.pdf

8 http://www.privacycommission.be/communiqu%E9s/AV37-2006.pdf

9 SWIFT letter to Chairman of the Article 29 Working Party of 31 July 2006.

10 **SWIFT Annual report 2005; available at http://www.swift.com/index.cfm?item_id=59684 .**

1.2.2. Categories of data processed

The messages that are transmitted via the SWIFTNet FIN service contain personal data such as the names of the beneficiary and the ordering customer. Payment related messages may however include more information such as a reference number to allow payer and payee to reconcile the payment with their respective accounting documents. In addition, certain message types allow for unstructured text information to be included.

Apart from sales offices in various countries, SWIFT has two operation centres located in SWIFT branches, one in a Member State of the EU and one in the United States. In these operation centres, as part of the SWIFTNet FIN service, all messages processed by SWIFT are stored and mirrored for 124 days, as a "back-up recovery tool" for customers in case of disputes between financial institutions or data loss. After this period the data is erased.

1.2.3. Subpoenas by the UST

Since the terrorist attacks of September 2001, the UST has addressed multiple administrative subpoenas to the SWIFT operation centre in the US. After enquiry, SWIFT stated that to date it had received and complied with 64 UST subpoenas.

Under US law, an administrative subpoena is an order from a government official to a third party, instructing the recipient to produce certain information.[11] The scope of the UST subpoenas in this case is materially, territorially and in time very wide and is defined in the subpoenas and in the correspondence on the negotiations between the UST and SWIFT. These subpoenas are issued for any transactions which relate or may relate to terrorism, relate to *x* number of countries and jurisdictions, on *y* date, or "*from ... to ...*" dates ranging from one to several weeks, within and outside the US. It concerns messages of inter-bank transactions within the US, to or from the US, as well as messages from outside the US, such as messages within the EU.[12]

SWIFT privately negotiated an arrangement with the US Treasury on how to comply with the subpoenas. Through this process, SWIFT claims to have received *"significant protections and assurances as to the purpose, confidentiality, oversight and control of the limited sets of data produced under the subpoenas"* [13].

According to the findings of the Belgian DPA, the practical communication of personal data to the UST is performed by the SWIFT operating centre in the US in several steps. There is no direct extraction of individualised data mirrored in the SWIFT database, but instead, SWIFT negotiated a "black box" construction with the UST that permitted a

---

[11] Hearing before the United States Senate Judiciary Committee, Subcommittee on Terrorism, Technology and Homeland Security:"Tools to Fight Terrorism: Subpoena Authority and Pretrial Detention of Terrorists" Testimony of Rachel Brand, Principal Deputy Assistant Attorney General, Office of Legal Policy, U.S. Department of Justice, June 22, 2004; http://kyl.senate.gov/legis_center/subdocs/062204_brand.pdf

[12] Cf. Opinion Belgian DPA, B.2 (unofficial EN translation), footnote 8.

[13] "SWIFT statement on compliance policy", published on http://www.swift.com/index.cfm?item_id=59897.

transfer of data from the mirrored SWIFT database to the "black box". Once the data are in the "black box", which is owned by the US, the UST performs focused searches.

Further details on the communication of personal data to the UST were disclosed to the DPA in Belgium and can be found in its opinion[14].

2. APPLICABLE DATA PROTECTION FRAMEWORK

2.1. Applicability of Directive 95/46/EC

Since personal data are contained in the messages that are transmitted via the SWIFTNet FIN service, the Working Party finds that the Directive is applicable to the processing of personal data via the SWIFTNet FIN service.

The Working Party stresses that the fact that the processing of personal data is incidental to the provision of a service is not relevant to the determination of an organisation's capacity as a data controller. The definitions of "processing of personal data" and "personal data" are clearly defined in Article 2 of Directive. Where the activities carried out by an entity fall under these definitions, the Directive applies and therefore the data processing activities shall be carried out in full conformity with the Directive.

2.2. Law applicable to SWIFT

Article 4(1)(a) of the Directive states that each Member State shall apply the national provisions it adopts pursuant to the Directive to the processing of personal data where "(...) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State".

The head office of SWIFT is located in La Hulpe, Belgium. SWIFT also has two operating centres (one in Europe and one in the US, which act as a complete mirror). In addition, SWIFT has several sales offices in the UK, France, Germany, Italy, Spain, etc. The critical decisions on the processing of personal data and transfer of data to the UST were decided by the head office in Belgium.

As a consequence, the processing of personal data by SWIFT is subject to Belgian law, implementing the Directive, regardless of where the data processing takes place.

2.3. Law applicable to the financial institutions

With regard to the processing operations for which the financial institutions which make use of SWIFT's service for their international payment orders can be considered as controllers, the applicable national law is determined by Article 4(1)(a) of the Directive and, with regard to Community institutions and bodies, Article 3 of Regulation (EC) 45/2001[15]. This means that, in the case of financial institutions, different – though harmonized – laws are applicable.

---

[14] See footnote 8.

[15] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data; OJ L 8, 12.1.2001, p. 1.

The Working Party stresses that, since personal data are being processed in financial transactions regarding hundreds of thousands of citizens via institutions established in the EU (the cooperative SWIFT as well as financial institutions making use of the SWIFTNet FIN service), the national laws on data protection – adopted in implementation of the Directive – of the different Member States concerned are applicable.

3. ROLE OF SWIFT AND OF THE FINANCIAL INSTITUTIONS

According to the Directive, the controller has to ensure that the obligations with respect to the processing of personal data are complied with.

The question is whether SWIFT and/or the financial institutions are to be considered as data controllers or as processors.

According to the definitions of the Directive, 'controller' means "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" (Article 2 (d));a 'processor' means "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (Article 2 (e)).

3.1. Role of SWIFT

SWIFT has always presented itself as being "*solely a messaging intermediary for transmitting secure and confidential financial messages between financial institutions. SWIFT is not a bank, nor does it hold accounts of any customers.*" This presentation also formed the basis for the assessments carried out by some DPAs in Member States when authorizing data processing activities by their banks.

The international service structure of SWIFT and the contractual arrangements that have been made between SWIFT and financial institutions are rather complex. The Working Party points out, however, that this type of structure including the role of a service provider working together with other actors is not unique. The SWIFT structure appears to be an example of a formal cooperative network. SWIFT was organized in 1973 by a group of European banks which wanted to develop a new method to send payment instructions to correspondent banks in a standardized manner. To this effect, a cooperative company with limited liability was established under Belgian law.

The Working Party refers to similar cases of cooperative networks such as the case of the Terminated Merchant Databases that are operated by VISA and Mastercard in cooperation with financial institutions in order to analyze the risks associated with signing up a particular merchant with the VISA or Mastercard system[16]. The Working Party also makes reference to the cases of clearing and settlement of transactions systems and to passenger reservation systems where travel agencies and airline companies on the one hand and the managers of those systems (such as Galileo) on the other hand have differing responsibilities.

---

[16] See e.g. Article 29 Working party "Guidelines for Terminated Merchant Databases"; available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/others/2005-01-11-fraudprevention_en.pdf.

Independently of the contractual relationship between SWIFT and the financial institutions under civil or commercial law, which may include the term "subcontractor", from the point of view of data protection, SWIFT is not a simple "subcontractor" or processor within the meaning of Article 2 of the Directive for the normal processing of personal data for its usual commercial purpose. The facts illustrate that SWIFT has evolved in the last few decades and does more than just act on behalf of its clients. Even if it was assumed for a moment that SWIFT acted as "processor", SWIFT has taken on specific responsibilities which go beyond the set of instructions and duties incumbent on a processor and cannot be considered compatible with its claim to be just a "processor".[17] The management of SWIFT operates in the context of a formal cooperative network which determines both the purposes and the means of data processing within the SWIFTNet Service and what personal data is processed via that service. The management of SWIFT decides autonomously on the level of information that is provided to the financial institutions in relation to the processing. SWIFT management is able to determine the purposes and means of the processing by developing, marketing and changing the existing or new SWIFT services and processing of data, e.g. by determining standards applicable to it clients as to the form and content of payment orders, without requiring the consent of the financial institutions. SWIFT also provides added value for the processing of personal data, such as the storage and validation of personal data and the protection of personal data with a high security standard. SWIFT management has the power to take critical decisions with respect to the processing, such as the security standard and the location of its operating centres. Finally, SWIFT management negotiates and terminates with full autonomy its services agreements and drafts and changes its various contractual documents and policies[18]. The above are the practical and legal means of the processing.

For the transfer of personal data to the UST, SWIFT decided to comply with the US subpoenas. It also took the initiative to negotiate in a non-transparent manner, through correspondence and a comfort letter with the UST, the conditions for passing the personal data to the UST. It deliberately decided not to inform the financial institutions concerned of this negotiation. Indeed, the control mechanisms obtained and operated by SWIFT affected the purpose and scope of the transfer of data to the UST. These actions exceed by far the normal capacities of a data processor in view of its supposed absence of autonomy with respect to the instructions of the data controller.

While SWIFT presents itself as a data processor, and some elements might suggest that SWIFT has acted in the past as a processor in certain cases on behalf of the financial institutions, the Working Party, having considered the effective margin of manoeuvre it possesses in the situations described above, is of the opinion that SWIFT is a controller as defined by Article 2 (d) of the Directive, for both the normal processing of personal data under its SWIFTNet service as well as for the further processing by onward transfer of personal data to the UST.

---

17 Data processors must in any case comply with the Directive, see e.g. Art. 17 (3) on security measures.

18 Cf. clause 4.5.3 of the general terms and conditions states: "the customer shall have been deemed to have consented to any such processing…".

3.2. Role of the financial institutions

The role of the financial institutions in the use of the SWIFTNet FIN service needs to be assessed. Some financial institutions were not fully informed by SWIFT of the volume and exact characteristics of the processing and mirroring of the personal data, including the further transfer of the mirrored personal data to the UST, However, after the disclosure of these facts on and after 23 June 2006, all financial institutions are aware of the situation when sending personal data via the SWIFTNet FIN service for international money transfers.

Financial institutions using SWIFT are supposed and expected to retain some influence on the policy of the cooperative. Some financial institutions are present on SWIFT's Board of Directors and the current management structure of SWIFT was originally designed to enable banks and financial institutions to retain some power over SWIFT decision-making processes. These institutions should therefore be considered as taking part in the determination of the purpose and means of the processing, with the cooperative of which they are members. They have also direct contact with the concerned natural persons, and they play an essential role in the execution of the international payment orders of their clients.

It is also important to keep in mind that the financial institutions are autonomous and that they can pursue their own objectives at an inter-bank level. The Working Party notes that, within the inter-bank traffic, the financial institutions often make crucial decisions on the transmission of personal data to SWIFT, often without the knowledge of their clients. This is shown by the following elements:

- On the inter-bank level, the financial institutions often decide autonomously about the means used when settling payment instructions. They can use or develop alternative or rival services for the transmission of these financial messages within the inter-bank system (e.g. e-mail, fax, telephone). Choices at this level will determine the global privacy characteristics regarding payment instructions settled by the financial institutions. When choosing an inter-bank service, the financial institutions are, in view of the diversity of the services at inter-bank level, free to be guided by elements other than information security - which is of course always a requirement - such as, the privacy policy of the professional service provider. The financial institutions have the option to use a strict privacy policy from a particular provider or use a solution such as virtual private network as a guarantee in order to safeguard the trust of their clients and their services to the maximum.
- Financial institutions adhere to and accept the contractual framework of the SWIFTNet FIN service[19]. The contractual documentation (Data Retrieval Policy[20]), and the SWIFT compliance policy make SWIFT customers aware of

---

[19] Part of the contractual documentation is the "SWIFT User Handbook" which contains the standardised message types to be used.

[20] Where it is stipulated: "*For the avoidance of any doubt, nothing in this policy or, more generally, SWIFT's obligations of confidence to customers, shall be construed as preventing SWIFT from retrieving, using, or disclosing traffic or message data as reasonably necessary to comply with a bona fide subpoena or other lawful process by a court or other competent authority.*" Cf. Opinion Belgian DPA, D.2, footnote 8.

the general principle to transfer personal data subjected to subpoenas either served on them or on SWIFT. According to the Opinion of the Belgian DPA, SWIFT argued that the number of subpoenas addressed to financial institutions could run into thousands or even tens of thousands per year. It is therefore doubtful that financial institutions which are active on the international payments market would be unaware of the general principle of subpoenas.

- The financial institutions must assess the possible implications and privacy risks, including privacy risks for their clients relating to the SWIFTNet FIN service, which they, as a professional service provider, sign up to. It is therefore important to check whether the privacy policy of the instructing institution contains clauses relating to these risks.
- Considering the fact that the financial institutions are acting on behalf of their clients giving payment instructions, they are not allowed to pass on the necessary data to other purposes than strictly payment transfer. If it is known to a financial institution, that SWIFT uses data entrusted to them also in ways which are not strictly payment transfers and nevertheless continues to make use of the SWIFT services, the question of the legal basis for such transfer and use must be put: unless there is a special agreement between financial institution and their clients it does not seem justified to entrust banking data to SWIFT for other purposes than the mere service acknowledged.

As a consequence, financial institutions are not only controllers in the meaning of Article 2 (d) of the Directive as to their own data processing activities but they also bear some responsibility as regards the data processing activities of SWIFT. The fact that the management structure of the SWIFT cooperative appears to have evolved over time to the point that SWIFT's management would have grown more independent than originally intended does not prevent its founders, i.e. the financial institutions, from retaining their qualification as data controllers in the sense of the Directive.

On the basis of the above elements, the Working Party is of the opinion that sufficient elements support the opinion that a joint responsibility exists with the financial institutions and the cooperative SWIFT where they are represented, for the processing of personal data via the SWIFTNet FIN service. However joint responsibility does not necessarily mean equal responsibility. Whilst SWIFT bears primary responsibility for the processing of personal data in the SWIFTNet FIN service, financial institutions also bear some responsibility for the processing of their clients' personal data in the service.

3.3. Role of central banks

The involvement of central banks must be examined, taking account of the different roles they play as regards SWIFT and as regards the oversight within the area of financial payments. Firstly, SWIFT is subject to cooperative oversight by the Central Banks of the Group of Ten countries (G-10 Group)[21]. The oversight focuses primarily on ensuring that SWIFT has effective controls and processes to manage risks for the financial stability

[21] The G-10 Group is composed by the National Bank of Belgium, Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d' Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System (USA), represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.

and the soundness of financial infrastructures. Furthermore, "overseers review SWIFT's identification and mitigation of operational risks, and may also review legal risks, transparency of arrangements and customer access policies. SWIFT's strategic direction may also be discussed with the Board and senior management"[22]. The major instrument for the oversight of SWIFT is the influence and pressure that may be applied by the overseeing authority ("moral suasion"). Overseers can formulate recommendations to SWIFT; however, it is also clear that the oversight of SWIFT does not grant SWIFT any certification, approval or authorisation by the Central Banks.

Provisions on the confidential treatment of non-public information are included in Memorandums of Understanding between SWIFT and the Central Banks.

The G-10 Group was informed in the course of 2002 about the data transfers to US authorities. However, the Group considered that this issue fell outside the scope of its oversight role. Furthermore, many central banks interpreted Memorandums of Understanding on confidentiality as preventing them from referring this issue to competent authorities at national and European level. Therefore, the G-10 Group neither addressed the consequences on data protection of the transfers to US authorities, nor did they inform the relevant authorities nor did they urge SWIFT to do so.

Furthermore, the President of the European Central Bank (ECB) stated at the public hearing at the European Parliament that the G-10 Central Banks "*did not give SWIFT any blessing in relation to its compliance with these subpoenas. In fact, we could not have given any such authorisation even if we had wanted to, as this fell outside our competence. Therefore, SWIFT remained solely responsible for its decisions*".[23]

Secondly, it shall be highlighted that the limited role that the Central Banks currently play in SWIFT oversight does not exclude that also a Central Bank might be considered – as any other financial institution using SWIFTNet service – as a (joint) controller whenever it acts as a SWIFT customer (see above, paragraph 3.2), in the event that they process personal data for the purpose of inter-bank transactions. In this perspective, the fact that some Central Banks were informed of the data transfers to US authorities might be considered as relevant in order to determine their responsibility as users of the SWIFT system.

4. ASSESSMENT OF THE COMPATIBILITY WITH DATA PROTECTION RULES

4.1. Application of the principles of data quality and proportionality (Article 6 of the Directive)

In accordance with Article 6 of Directive, personal data must be processed fairly and lawfully;[24] they must be collected for specified, explicit and legitimate purposes[25] and

---

[22] Financial Stability Review 2005, published by the National Bank of Belgium and available on its web site www.nbb.be.

[23] Jean-Claude Trichet: Statement by the President of the ECB at the public hearing at the European Parliament on the interception of bank transfer data from the SWIFT system by the US secret services.

[24] Article 6(1)(a) of the Directive.

not be processed for purposes incompatible with the original one for which they were collected. Moreover, the processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[26] Combined, these latter rules are referred to as the "proportionality principle". Finally, appropriate measures have to be taken to ensure that data which are inaccurate or incomplete are erased or rectified.[27]

4.1.1. Commercial purpose

The personal data was collected by the financial institutions only for the purpose of processing the client's payment orders and subsequently by SWIFT for the purpose of executing the SWIFTNet FIN service (commercial purpose). This commercial purpose for the processing of personal data can therefore be considered as the only specified, explicit and legitimate purpose.

As to the transfer of personal data to third countries, see below under section 4.6

4.1.2. Further processing for incompatible purposes

aa) Personal data may not be processed for purposes which are incompatible with the original purpose. By deciding to mirror all data processing activities in an operating centre in the US, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law.

In this case, SWIFT received subpoenas issued by the UST for alleged terrorism investigations. This further purpose is completely different from the original purpose and its treatment of the personal data involved, and may have direct consequences for the individuals whose personal data are being processed. This further purpose is not compatible with the original, commercial-only purpose for which personal data have been collected.

SWIFT was aware of this further purpose. The SWIFT management endorsed it and cooperated. SWIFT has not pointed this purpose out, neither to the users of its services nor to any data protection supervisory authority.

bb) It has also been established that massive data transfers took place from SWIFT to the UST, without an effective possibility to check the individualized character of the data requested. According to SWIFT, all financial messages could potentially be scrutinized via the "black box" system by the UST. This system allows the UST to retrieve from the "black box" all messages – and the personal data contained therein – it deems necessary.

The Working Party points out that even for the purposes of alleged terrorism investigations only specific and individualized data should be transferred by SWIFT on a

---

[25] Article 6(1)(b) of the Directive.

[26] Article 6(1)(c) of the Directive.

[27] Article 6(1)(d) of the Directive.

case by case basis, in full compliance with data protection principles. As this is not the case, the current practice is not proportionate and thereby violates Article 6 (1) (c) of the Directive.

cc) Article 13 provides that "Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6(1) [as the purpose limitation principle], 10, 11(1) [duty to inform the data subject], 12 [right of access] and 21 [publicizing of processing operations] when such a restriction constitutes a necessary measure to safeguard [a list of important public interests which follows] (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences [...]; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);".

The European Court of Justice (ECJ) has cast some light on the understanding of these provisions. On joined cases C-465/00, C-138/01 and C-139/01 ("Rechnungshof") of 20 May 2003, the Court made clear that the communication of data originally collected for "economic" purposes to third parties, including public authorities "constitutes an interference within the meaning of Article 8 ECHR". Further, derogations from the principle of purpose limitation laid down in the Data Protection Directive need to respect Article 13 of that directive, and for that they need to be "justified from the point of view of Article 8 of the Convention" (Rechnungshof, C-465/00, §68 ff).

According to the Convention, in order for an interference with the right to private life to be justified, it needs to be done "in accordance with the law" and be "necessary in a democratic society" for a public interest purpose. The Strasbourg jurisprudence has repeatedly reminded that the Law providing for the interference "must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference."

However, these provisions cannot be invoked as SWIFT did not comply on these issues with the Belgian law.[28]

dd) The Working Party moreover points to the existence of legal structures on governmental level. The Working Party emphasizes that systems should be used in compliance with the bank secrecy principle. It refers in this respect to the 40+9 **recommendations of the Financial Action Task Force (FATF/GAFI), an inter-governmental body created in 1989 whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The Working Party also refers to the system of exchange of financial information put in place between the respective national financial intelligence cells of 96 countries (Egmont Secure Web, ESW), coordinated by FinCEN in the United States. In this framework, financial information can be given to the requesting party in compliance with the national rules of the country exporting the information.**

---

[28] Opinion Belgian DPA, cf. footnote 8.

The Working Party also refers to existing cooperation mechanisms set up or developed under the third pillar (judicial and police cooperation), and in particular the international agreements signed on 25 June 2003 between the US and the EU[29] on mutual legal assistance and, although more remotely to this subject, the international agreement on extradition. Although these treaties are not yet ratified, according to Article 18 of the Vienna Convention on the Law of Treaties[30], a State is obliged to refrain from acts which would defeat the object and purpose of a treaty when it has signed the treaty or has exchanged instruments constituting the treaty subject to ratification, as long as it has not notified an intention not be become a party to the treaty.

As a result by having decided to mirror all data processing activities in an operating centre in the US, SWIFT placed itself in a foreseeable situation where it is subject to subpoenas under US law and where a processing of personal data has been organized in a way that appears to circumvent the structures and international agreements already in place.

Overall, the Working Party is of the opinion that the principles of purpose limitation and compatibility, proportionality and necessity of the personal data processed are not respected.

4.2. Legitimacy (Article 7 of the Directive)

For any personal data processing to be lawful, it needs to be legitimate and satisfy one of the grounds set out in Article 7 of the Directive.

4.2.1. Necessary for the performance of a contract (Article 7 (b) of the Directive)

SWIFT processes the personal data contained in the messages in the SWIFTNet Fin service in order to execute payment orders entrusted to SWIFT by the financial institutions only.

However, even if in this context such processing for this commercial purpose could be considered necessary for the execution of the agreement between SWIFT and the financial institutions concerned, the way it was done by mirroring the personal data in the US operations centre is not acceptable for other reasons which are discussed later at 4.6 .

4.2.2. Necessary for compliance with a legal obligation to which the controller is subject (Article 7(c) of the Directive)

The processing and mirroring could have been necessary for compliance with a legal obligation to which the controller is subject.

---

[29] Agreement on extradition between the EU and the US" and the "Agreement on mutual legal assistance between the EU and the US". http://eur-lex.europa.eu/LexUriServ/site/en/oj/2003/l_181/l_18120030719en00270033.pdf and http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_181/l_18120030719en00340042.pdf#search=%22Agreement%20on%20mutual%20legal%20assistance%20between%20the%20european%20union%22

[30] Treaty of Vienna on the law of treaties of 23 May 1969. The United States have signed this treaty.

SWIFT, with its headquarters in Belgium, did not formally invoke a legal basis within Belgian or European law for this particular processing. The Working Party further notes that is no legal obligation imposed by Belgian or European law for this particular data processing activity. In addition, the Working Party already stated in its "SOX opinion"[31] that *"an obligation imposed by a foreign legal statute or regulation (...) may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate. Any other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in Directive"*. The Working Party considers that this reasoning also fully applies in this case.

Article 7 (c) of the Directive can therefore not be used to justify the processing and mirroring of the personal data in this case.

4.2.3. Necessary for the purposes of a legitimate interest pursued by the controller (Article 7(f) of the Directive)

According to Article 7(f) of the Directive, the processing and mirroring could be necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

The question is whether Article 7 (f) of the Directive could be used to justify the processing and mirroring, with the consequence that the processing operations in its US operations centre are subject to US subpoenas.

It cannot be denied that SWIFT has a legitimate interest in complying with the subpoenas under US law. If SWIFT did not comply with these subpoenas, it runs the risk of incurring sanctions under US law. On the other hand, it is also crucial that a "proper balance" is found and respected between the risk of SWIFT being sanctioned by the US for eventual non-compliance with the subpoenas and the protection of the rights of individuals.

Article 7 (f) of the Directive requires a balance to be struck between the legitimate interest pursued by the processing of personal data and the fundamental rights of data subjects. This balance of interest test should take into account issues of proportionality, subsidiarity, the seriousness of the alleged offences that can be notified and the consequences for the data subjects. In the context of the balance of interest test, adequate safeguards will also have to be put in place. In particular, Article 14 of the Directive provides that, when data processing is based on Article 7(f), individuals have the right to object at any time on compelling legitimate grounds to the processing of the data relating to them.

---

[31] Opinion 1/2006 on the application of the EU data protection rules to internal wistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against, banking and financial crime.

SWIFT conducted the processing and mirroring of its data in a "hidden, systematic, massive and long-term"[32] manner, without having specified the further incompatible purpose at the time of processing the data, and without SWIFT pointing this purpose out to the users of its services. This further processing and mirroring for an incompatible purpose could have far-reaching effects on any individual.

The Working Party therefore considers that the interests for fundamental rights and freedoms of the numerous data subjects override SWIFT's interest not to be sanctioned by the US for eventual non-compliance with the subpoenas.

4.3. Provision of clear and complete information about the scheme (Articles 10 and 11 of the Directive)

According to Articles 10 and 11 of the Directive, the controller is obliged to inform data subjects about the existence, purpose and functioning of its data processing, the recipients of the personal data and the right of access, rectification and erasure by the data subject. All clients of financial institutions, regardless of their nationality or country of residence, have a right to know what happens to their "confidential" data.

The Working Party observes that this information concerning the processing and mirroring in the US operations centre was not provided, neither by SWIFT, nor by the financial institutions concerned.

According to Article 13 of the Directive, EU Member States may adopt legislative measures to restrict the scope of some of the obligations and rights provided for in the Directive. Such a restriction must constitute a necessary measure to safeguard, e.g. the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions, on a case-by-case basis and only if that interference is justified from the point of view of Article 8 of the European Convention of Human Rights. However such a general, long and large-scale operation without any information provided at all would not be in line with Article 13.

4.4. Compliance with notification requirements (Article 18 to 20 of the Directive)

Data controllers have to comply with the requirements of Articles 18 to 20 of the Data Protection Directive as regards notification of their data processing activities to, or prior checking by, the national data protection authorities.

In Member States providing for such a procedure, the processing operations might be subject to prior checking by the national data protection authority in as much as those operations are likely to present a specific risk to the rights and freedoms of the data subjects. The evaluation of whether such processing operations fall under prior checking requirements depends on the national legislation and the practice of the national data protection authority.

---

[32] Opinion Belgian DPA, cf footnote 8.

The Working Party notes that SWIFT did notify some types of processing to the Belgian DPA[33] but did not notify the processing and mirroring in the US operations centre for the execution of international payment orders and neither the further purpose.

4.5. Oversight mechanisms

The establishment in EU Member States of data protection supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data. This principle of complete independence of the supervisory authority is laid down in Article 28 of the Directive.

Due to the lack of information by SWIFT, the financial institutions and the overseers to the national data supervisory authority, the existing data protection control mechanisms of the Directive could not be effectively applied. The Working Party regrets that no prior consultation, formal or informal, was effected by SWIFT or the financial institutions with the data protection authorities in relation to the processing and mirroring of personal data in the US operations centre.

Verifications by the national authorities show that for the transfer of SWIFT data to the UST for the further purpose the control measures that were put in place by SWIFT mainly consisted of private audit controls by a consultant company, and the review by SWIFT employees ("scrutinizers") which, for security reasons, were not allowed to report details of the findings internally. SWIFT also mentioned that it is overseen by a senior committee drawn from the G-10 central banks and that SWIFT has informed the overseers of this matter.

Although the control measures put in place by SWIFT may contribute to enhance the security of the data processing activities, the Working Party strongly insists that no other mechanism provided for by data controllers can replace the control of data processing activities by a public independent supervisory authority as required by Article 28 of the Directive. In any case, the oversight group set up by the G-10 central banks declared itself incompetent to examine any question relating to the protection of personal data.

As a result, the Working Party condemns the fact that the existing mechanisms for independent control by the public supervisory authorities of personal data processing have been circumvented for the personal data processed via the SWIFTNet FIN service.

4.6. Transborder data flows (Articles 25 and 26 of the Directive)

Articles 25 and 26 of the Directive apply where personal data are transferred to a third country. Any transfer of data generated within EU territory that is to be used outside EU territory has to be subject to an adequacy assessment pursuant to the Directive. Furthermore, the provisions of the Directive relating to transfers of personal data to third countries cannot be applied separately from other provisions of the Directive. As explicitly mentioned in Article 25(1), these provisions apply "without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive". This means that regardless of the provisions relied upon for the purpose of

---

[33] Opinion Belgian DPA, cf. footnote 8.

data transfer to a third country, other relevant provisions of the Directive need to be respected[34].

The normal functioning of the SWIFTNet FIN service includes a continuous and massive transborder data flow, due to the location of the SWIFT operating centres. The SWIFT operating centres are not separate legal entities, but branches ("*succursales*") of the cooperative company established under Belgian law. The store-and-forward capability of the two SWIFT operating centres in Europe and in the US operates as follows: The messages are decrypted automatically in the operating centres to store and forward the information in a few milliseconds. This "store-and-forward" process is intended to validate (control the correctness or the presence of letters/numbers in the mandatory message fields) the information (for instance make sure that the correct currency code of the transfer is filled in, e.g. "EUR") on the basis of contents that is standardized. During this process, the information is also stored for 124 days in both operating centres for security (back-up) reasons which then act as perfect "mirrors". This ensures that the data storage is parallel and the data are identical.

For SWIFT to lawfully process and mirror personal data in the US it needs first for these data to be transferred from the EU pursuant to Belgian law adopted in accordance with the Directive, in particular Articles 25 and 26 on the transfer of personal data to third countries. The transfers by SWIFT to the United States therefore have to be considered taking account of two elements: firstly, the commercial processing and mirroring of personal data by SWIFT Belgium to its operating centre in the US, and secondly, the processing of the data for the further purpose by the UST as agreed to by SWIFT.

4.6.1. Adequate data protection (Article 25 (1) of the Directive)

According to Article 25 (2) of the Directive, the adequacy of the level of protection afforded by a third country "shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country."

Taking into account the above criteria and applying the principles defined in Working Document WP12[35], the Working Party finds that in the USA currently only the "Safe Harbour" scheme provides for an adequate level of protection for data transfers from the EU to US organisations having joined this scheme. However, it does not cover financial services[36],.

---

[34] Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. WP 114.

[35] "Transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive", adopted by the Working Party on 24 July 1998; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf.

[36] cf. http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

Therefore, as a Belgian legal entity, SWIFT could not rely on Article 25 of the Directive for the processing and mirroring in the US operations centre.

4.6.2. Adequate safeguards put in place by recipient (Article 26 (2) of the Directive)

Under Article 26(2) of the Directive a Member State may also authorise a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection where the data controller offers "*adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights*". The end of Article 26(2) also states that these safeguards "*may in particular result from appropriate contractual clauses*". To facilitate the use of contractual clauses, the European Commission has issued three decisions on standard contractual clauses, two of which regulate transfers from a data controller to a data controller while the third regulates transfers from a data controller to a processor[37]. In addition, apart from the possibility of using contractual clauses to provide such sufficient safeguards, since 2003 the Article 29 Working Party has been working actively on the possibility of multinational groups using "binding corporate rules" for the same purpose[38].

However, in this case, SWIFT has not made use of these possibilities for its processing and mirroring in the US operating centre.[39]

4.6.3. Derogations (Article 26 of the Directive)

Article 26(1) of the Directive states that transfers of personal data to a third country which does not ensure an adequate level of protection may take place if one of the following conditions listed under (a) to (f) is met. As previously indicated by the Working Party in its working document WP12[40] mentioned above, the interpretation of Article 26(1) must necessarily be strict.

In this respect, the Working Party emphasises that this logic is the same as that of the additional protocol to Council of Europe Convention 108. The report on this protocol states that "the parties have discretion to determine derogations from the principle of an adequate level of protection. The relevant domestic provisions must nevertheless respect

---

37 As regards transfers from a data controller to a data controller, the Commission issued a first set of standard contractual clauses on 15 June 2001; it subsequently amended this decision in order to annex a new set of alternative clauses (decision of 27 December 2004). With regard to transfers from a data controller to a processor, the Commission issued a set of standard contractual clauses on 27 December 2001. All these clauses are available on the following website: http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_en.htm.

38 Cf. Working document WP 74, "Transfers of personal data to third countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" adopted by the Working Party on 3 June 2003 and further complementary documents WP107 and WP108.

39 In any case, if SWIFT were to make use of these possibilities, the Article 29 Working Party recalls that for any onward data transfer derogations from the applicable data protection law may not go beyond the restrictions necessary in a democratic society.

40 Cf. footnote 35, above.

the principle inherent in European law that clauses making exceptions are interpreted restrictively so that the exception does not become the rule".[41]

The possible derogations in this case are as follows:

4.6.3.1. Consent of the data subject (Article 26 (1) (a) of the Directive)

For this derogation to be lawfully invoked, the data subject must give his/her consent unambiguously to the proposed transfer. As already indicated in the Working Party's previous working document WP 12 this consent, whatever the circumstances in which it is given, must be a freely given, specific and informed indication of the data subject's wishes, as defined in Article 2(h) of the Directive.[42] The data subject must be informed of the transfer to a third country without an adequate level of protection or without having put in place the appropriate safeguards and can then decide whether he will run the associated risk or not.

SWIFT has not obtained the unambiguous consent of the data subjects for the processing and mirroring in the US operating centre and therefore cannot rely on Article 26 (1) (a) of the Directive.

4.6.3.2. Transfer is necessary for performance of a contract between the data subject and the controller or for the implementation of precontractual measures taken in response to the data subject's request (Article 26 (1) (b) of the Directive)

This exception means that the data transferred must be truly necessary to the purpose of the performance of this contract or of these precontractual measures. For this reason, the Working Party takes the view that this condition could not be applied to transfers of data by SWIFT to the US operating center, as SWIFT does not have a direct contractual relationship with the individual. Also, this derogation cannot be applied to transfers of additional information not necessary for the purpose of the transfer, or transfers for a purpose other than the performance of the contract. More generally, the derogations of Article 26(1)(b) to (e) only allow that the data which are necessary for the purpose of the transfer may be transferred on the basis of the individual derogations; for additional data, other means of adducing adequacy should be met.

4.6.3.3. Transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party (Article 26 (1) (c) of the Directive)

Likewise the derogation under Article 26(1)(b), a transfer of data to a third country which does not ensure adequate protection cannot be deemed to fall within the exception contained in Article 26(1)(c) unless it can be considered to be truly "necessary for the conclusion or performance of a contract between the data controller

---

41 Cf. report on the Additional Protocol to Convention 108 on the control authorities and cross border flows of data, Article 2(2)(a); this document can be accessed at:

http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm

42 Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. WP 114.

and a third party, in the interest of the data subject", and pass the corresponding "necessity test". **This test requires a close and substantial connection between the data subject's interest and the purposes of the contract.**[43]

The Working Party takes the view that this condition may not be applied to transfers of data by SWIFT to the US operating centre.

4.6.3.4. Transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims (Article 26 (1) (d) of the Directive)

SWIFT stated that the mirroring of processing data to the operations centres was considered as a critical element in the global financial system and that this mirroring of processing had been proposed by the overseers (G-10 central banks) for security reasons and reliability, and that SWIFT infrastructure would be considered critical for the global financial industry. SWIFT argues that this ground would justify the transfer on the basis of Art. 26(1)(d) of the Directive.

The Working Party cannot follow this interpretation. Even if it would be established that international mirroring of the processing (on a different continent other than Europe) would be "necessary or legally required on important public interest grounds" in the meaning of Article 26(1)(d) of the Directive, it is always possible to mirror such a processing outside the EU or EEA in a country that would provide an adequate level of protection. The Working party refers to countries such as Argentina[44] or Canada[45], that, according to European Commission Decisions, are considered as satisfying the requirements of the Directive. The "mirroring" in a non-EU country without an adequate level of data protection was is not necessary and cannot be justified by Article 26(1)(d).

Furthermore, personal data, collected and processed via the SWIFT network for international money transfers using the BIC or "SWIFT" code, and mirrored in the US, were provided to the UST since the end of 2001 on the basis of subpoenas under US law.

The full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, investigation, detection and prosecution of money laundering and the financing of terrorism and has been subject to regulation under EU law[46].

The Working Party recognizes that the fight against terrorism constitutes a legitimate purpose of the democratic societies in the interest of the safety of the state and that to this end measures can be taken which interfere with the fundamental right to personal data protection. The Working Party recalls its full commitment in this respect. It also

---

[43] Article 29 Working Party: Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995. WP 114

[44] Commission Decision C(2003) 1731 of 30 June 2003; OJ L 168, 5.7.2003.

[45] Commission Decision 2002/2/EC of 20.12.2001 on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act; O.J. L 2/13 of 4.1.2002.

[46] E.g. Regulation of the European Parliament and of the Council on information on the payer accompanying transfers of funds, adopted on 8 November 2006, not yet published; initial Commission Proposal COM (2005) 343.

considers that international instruments do provide for an appropriate legal framework enabling international cooperation. To this end, the Working Party is of the opinion that the possibilities already offered by current international forms of cooperation set up in respect of the fight against terrorism and terrorism investigation should be exploited while ensuring the required level of protection of fundamental rights.

The Working Party notes nevertheless that Article 26 (1)(d) of the Directive does not apply either as the transfer is not necessary or legally required on important public interest grounds of a EU Member State (Belgium). On this point the drafters of the Directive clearly did envisage that only important public interests identified as such by the national legislation applicable to data controllers established in the EU are valid in this connection. Any other interpretation would make it easy for a foreign authority to circumvent the requirement for adequate protection in the recipient country laid down in the Directive.

4.6.3.5. Transfer is necessary in order to protect the vital interests of the data subject (Article 26 (1) (e) of the Directive)

This exception applies to transfers that must relate to the individual interest of the data subject and, when it bears on health data, it must be necessary for an essential diagnosis. Accordingly, this exception could not be used to justify transferring personal medical data for a purpose such as general medical research.[47]

SWIFT has not claimed that the transfer is necessary in order to protect the vital interests of the data subjects for the processing and mirroring in the US operating centre. The Working Party considers that in any case this exception is irrelevant here. Article 26 (1) (e) of the Directive cannot be relied upon.

4.6.4. Findings

SWIFT may have relied on Article 26 (2) of the Directive for making a legal transfer of personal data to its operating centre in the US. However, SWIFT decided to transfer personal data without having complied with the legal requirements under Belgian law for such international data transfers.

SWIFT cannot rely on any of the other exceptions of Article 26 of the Directive.

As for the processing and mirroring in the US, even the commercial processing and mirroring did not take place legally. The continuing processing and mirroring, considering its further incompatible purpose and its large scale does not fall within the boundaries of what is necessary in a democratic society and further prevents SWIFT from transferring the personal data to the US.

5. CONCLUSIONS:

On that basis, the Working Party is of the opinion that:

---

[47] Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_en.pdf.

5.1. The EU Data Protection Directive 95/46/EC is applicable to the exchange of personal data via the SWIFTNet FIN service;

5.2. SWIFT and the financial institutions bear joint responsibility in light of the Directive for the processing of personal data via the SWIFTNet FIN service, with SWIFT bearing primary responsibility and financial institutions bearing some responsibility for the processing of their clients' personal data.

5.3. SWIFT and the financial institutions in the EU have failed to respect the provisions of the Directive:

5.3.1. *SWIFT*: As far as the processing and mirroring of personal data in the framework of the SWIFTNet FIN service is concerned, SWIFT as a data controller must comply with its obligations under the Directive, amongst which are the duty to provide information, the requirement to notify the processing, the obligation to provide an appropriate level of protection in order to meet the requirements for international transfers of personal data;

5.3.2. *Financial institutions*: The financial institutions in the EU as data controllers have the legal obligation to make sure that SWIFT fully complies with the law, in particular data protection law, in order to ensure protection of their clients. The financial institutions are responsible for having sufficient knowledge of the different payment systems and their technical and legal characteristics and risks. If financial institutions did not strive (sufficiently) to obtain such knowledge, they would accept substantial legal and client risks in breach of their fundamental duty of care. In particular, if some services such as the SWIFTNet FIN service involve massive transfers to countries without adequate data protection in the light of the Directive or if it is likely that such transfers would pose specific privacy concerns or risks, the Working Party is of the opinion that it is essential that the individual clients of the financial institutions are informed by the financial institutions, as their providers of professional services, in accordance with the transparency requirements of the Directive.

5.4. The Working Party is of the opinion that the lack of transparency and adequate and effective control mechanisms that surrounds the whole process of transfer of personal data first to the US, and then to the UST represents a serious breach in light of the Directive. In addition, the guarantees for the transfer of data to a third country as defined by the Directive and the principles of proportionality and necessity are violated.

As far as the communication of personal data to the UST is concerned, the Working Party is of the opinion that the hidden, systematic, massive and long-term transfer of personal data by SWIFT to the UST in a confidential, non-transparent and systematic manner for years without effective legal grounds and without the possibility of independent control by public data protection supervisory authorities constitutes a violation of fundamental European principles as regards data protection and is not in accordance with Belgian and European law. An existing international framework is already

available with regard to the fight against terrorism. The possibilities already offered there should be exploited while ensuring the required level of protection of fundamental rights.

5.5. The Working Party recalls once again[48] the commitment of democratic societies to ensure respect for the fundamental rights and freedoms of the individual. The individual's right to protection of personal data forms part of these fundamental rights and freedoms[49]. The Community Directives on the protection of personal data (Directives 95/46/EC and 2002/58/EC) form part of this commitment[50]. These Directives aim to ensure respect for fundamental rights and freedoms, in particular, the right to privacy with regard to the processing of personal data and to contribute to the respect of the rights protected by Article 8 of the European Convention on Human Rights, and Article 8 of the EU Charter of Fundamental Rights. In all these instruments, exceptions to combat crime are provided for but have to respect specific conditions.

6. IMMEDIATE ACTIONS TO BE TAKEN TO IMPROVE THE CURRENT SITUATION:

In view of the above, the Working Party therefore calls for the following immediate actions to be taken to improve the current situation:

6.1. **Cessation of infringements:** SWIFT and the financial institutions shall comply with their legal obligations under national and European law. This includes taking steps to ensure that any transfers of personal data are in line with the law. In case of non-compliance, data controllers can expect to be subject to sanctions imposed by the competent authorities under the Directive and national law, in order to enforce compliance.

6.2. **Return to lawful data processing:** The Article 29 Working Party calls upon SWIFT and the financial institutions to immediately take measures in order to remedy the currently illegal state of affairs, and to return to a situation where international money transfers may be made in full compliance with data protection law. The Working Party welcomes the fact that some data protection authorities are already urging the financial institutions to find a solution without delay.

6.3. **Actions as regards SWIFT:** For all its data processing activities, SWIFT as a controller must take the necessary measures to comply with its obligations under Belgian data protection law implementing the Directive.

6.4. **Actions as regards Central Banks:** The present situation calls for a clarification of the oversight on SWIFT. The Working Party recommends

---

48 Article 29 Opinion 10/2001 on the need for a balanced approach in the fight against terrorism; http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm .

49 See in particular Art. 8 Charter of Fundamental Rights of the European Union as well as case-law of the European Court of Human Rights in the affairs "Aman" of 16 February 2000 and "Rotaru" of 4 May 2000.

50 See recitals 1, 2, 10 and 11 of Directive 95/46/EC.

that appropriate solutions are found in order to bring compliance in particular with data protection rules clearly within the scope of the oversight, without prejudice to the powers of national data protection supervisory authorities, as well as to ensure that relevant authorities are duly and timely informed where necessary. The Working Party considers that the lack of compliance with data protection legislation may actually hamper consumers' trust in their banks and might thus affect also the financial stability of the payment system (reputation risk). Legal obstacles such as professional secrecy obligations of the overseers that could be used as argument to limit the effective control by the independent data protection authorities, should not be relied upon in a case of possible violation of constitutional or human rights.

6.5. **Actions as regards Financial Institutions:** All financial institutions in the EU using the SWIFTNet Fin service including the Central Banks have to make sure that according to Articles 10 and 11 of the EU Directive 95/46/EC their clients are properly informed about how their personal data are processed and which rights the data subjects have. They also have to give information about the fact that US authorities might have access to such data. Data protection supervisory authorities will enforce these requirements in order to guarantee that they are met by all financial institutions on a European level and they will cooperate on harmonized information notices. The Article 29 Working Party recalls in this connection its opinion adopted on harmonized information provisions[51]. It also seems appropriate for financial institutions and Central Banks to consider alternative technical solutions to the procedures that are currently used, in accordance with the principles of the Directive.

The Working Party also stresses the following:

6.6. **Preservation of our fundamental values in the fight against crime:** The Working Party recalls that any measures taken in the fight against crime and terrorism should not and must not reduce standards of protection of fundamental rights which characterise democratic societies. A key element of the fight against terrorism involves ensuring the preservation of the fundamental rights which are the basis of democratic societies and the very values that those advocating the use of violence seek to destroy.

6.7. **Global data protection principles:** The Working Party considers it essential that principles for the protection of personal data, including control by independent supervisory authorities, are fully respected in any framework of global systems of exchange of information.

The Article 29 Working Party will follow-up and monitor all of the above.

---

[51] Article 29 Working Party "Opinion on More Harmonised Information Provisions", 25 November 2004. WP 100; http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp100_en.pdf.

Done at Brussels, on 22 November 2006

For the Working Party
The Chairman
Peter Schaar